EXHIBIT 15

Rebuttal Expert Report to Strike 3 Holding's Expert Reports of Paige and Bunting Regarding Reliability of the IPP Infringement Monitoring System

April 29th, 2019
Prepared by Dr. Kal Toth, P.Eng., Portland, OR 97205
For Mr. J. Curtis Edmondson, Law Offices of J. Curtis Edmondson, Hillsboro, OR 97124

In this report I rebut declarations and reports by the Plaintiff's experts (Paige and Bunting), relating their work to information disclosed by two members of IPP's operational staff. As indicated below I am of the opinion that the experts did not provide convincing facts, data, principles, methods, and reasoning demonstrating that the IPP system operates reliably for its intended purposes, namely to:

(a) detect and report infringement, and

(b) support the essential day-to-day procedures of verifying IPP system outputs by operational stafff.

The approach I have therefore taken is to first summarize the pertinent facts and data disclosed by way of the depositions of Stalzer and Pasquale, followed by discussions relating to the expertise and methods used by the Plaintiff's experts to test the operational IPP system.

Contents

1. My Approach

Below I describe operational scenarios highlighting pertinent facts, data and methods experts that Paige and Bunting have failed to address. These informational gaps imply there is a significant risk that IPP delivers an unacceptable number of false positive reports of infringement. By false positives I mean operational scenarios where data reported by the IPP system incorrectly binds an identifying attribute of a user, such as an IP address, with a copyrighted movie of the Plaintiff. More generally, I have defined:

> *false positives are undetected reports of infringement delivered to a plaintiff that could culminate in the issuance of a subpoena that wrongfully discloses the identity of an innocent party.*

Software and systems engineering professionals routinely apply best practices to ensure that the systems, software, and procedures they design and specify are reliable enough to minimize operational risks. To date, the Plaintiff's experts have not provided convincing facts and data showing that such best practices and have been applied to develop, test, quality assure, and maintain the IPP system. I understand that IPP is touted by some of IPP's experts to be a forensics tool that accurately identifies infringing BitTorrent users. I am of the opinion that IPP if cannot be relied upon to consistently discriminate between infringers and non-infringers, it should not be used for forensics purposes.

Should the Plaintiff's experts provide facts, data and method demonstrating that the system requirements are consistently satisfied by the operational system, I would gladly review and re-assess IPP's reliability (Exhibit 9).

I acknowledge that the false positive rates for complex systems are challenging to assess. I believe the burden of proof is on the owner of a forensics tool, such as IPP, to provide requisite facts, data, and methods that demonstrate that the system is sufficiently reliable to mitigate the risk of false positives being delivered.

2. Synopsis of My Qualifications

The opinions expressed in this report are drawn from my professional experience provided in the annex to my *Amended Expert Report: Reliability Assessment of IPP Software, Kal Toth, 04/15/19* (Exhibit 9). My most relevant qualifications include: independent validation and verification of a secure messaging network for Canada's embassies abroad; quality, reliability, maintainability, safety, security, and software engineering for Hughes Aircraft for Canada's air traffic control system; software engineering practice leader for CGI Group and Hughes Aircraft; and software engineering courses for ten universities including Portland State University, Oregon State University, and the Technical University of British Columbia (now part of Simon Fraser University).

3. Evidence Reviewed and Referenced

Exhibit 1 Declaration of Susan B. Stalzer in Support of Plaintiff's Motion for Leave to Serve a Third Party Subpoena Prior to Rule 26(f) Conference, Case No.: 2:17-cv-01731-MJP, Document 4-5, filed 11/29/17.

Exhibit 2 Extracted pages from the rough transcript of the deposition of Susan B. Stalzer deposition, 4/16/19, pp. 29, 33, 49, 58, 75, 76,118, 133, 138, 140, 141).

Exhibit 3 Declaration of John S. Pasquale in Support of Plaintiff's Motion for Leave to Serve a Third Party Subpoena Prior to Rule 26(f) Conference, Case No.2:17-cv-01731-MJP, Document 4-4, filed 11/29/17.

Exhibit 4 Extracted pages from the rough transcript of the deposition on John S. Pasquale, 04/17/19, pp25-28, 33-36, 37-38, 42-45, 53-54, 72-74.

Exhibit 5 Declaration of Patrick Paige, S3H (217-cv-01731)_000166, filed 11/12/13.

Exhibit 6 Expert Report Regarding Testing of IPP International UG's Infringement Detection System (Exhibit B), Patrick Paige Computer Forensics LLC, S3H (217-cv-01731)_000171, filed 11/06/18.

Exhibit 7 Declaration of Stephen M. Bunting, S3H (217-cv-01731)_000155, dated 12/11/18.

Exhibit 8 Declaration of Brandon Garcia-Paeth in Support of Defendant's Opposition to Plaintiff's Motion for Summary Judgment, Case no. 2:17-cv-01731-TSZ, 02/25/219.

Exhibit 9 Amended Expert Report: Reliability Assessment of IPP Software, Kal Toth, 04/15/19.

4. Video Verification, Susan Stalzer

Having reviewed declaration Exhibit 1 and deposition Exhibit 2 of Susan Stalzer, I can confirm the following:

a. Stalzer's declaration Exhibit 1 (paras 7 and 8) state that she was tasked to visually verify each *infringing file* provided to her by IPP to determine if it was identical to, strikingly similar to, or substantially similar to a motion picture (movie) identified as owned by Strike 3 on torrent websites;

b. Stalzer deposition Exhibit 2 discloses that she uses a *verification tool* to select and display from a list of movie titles on her computer screen, each having a hash mark, each representing a [purportedly] infringing file; and also displaying a copy of a movie owned by Strike 3 (control copy) obtained and displayed by logging into a torrent website, entering the same movie title into the search window of her browser, and downloading the file;

c. Stalzer in Exhibit 2 discloses that she uses the verification tool to select a file from the list, visually compares the two movies, and indicates whether they visually match ("good") or do not match ("bad") by pressing a button, recording failed matches ("bad") in an Excel spreadsheet. At some later date, she signs a declaration listing movies that she apparently identified as "good". With respect to her comparison task, Stalzer confirms (pp.140-141) that she does "not have a measure with which to grade between the three categories" [identical to, strikingly similar to, or substantially similar];

d. Apparently, Stalzer does not rely on the provided hashes to execute her task, and is not provided the IP address of purported infringer(s) via her verification tool. Her screen does not indicate that the infringed file was received from the IPP system or that the downloaded control copy of the movie is owned by Strike 3. The *verification tool* apparently interfaces with IPP and is not a commercial product;

5. PCAP Verification, John Pasquales

I reviewed declaration Exhibit 3 and deposition Exhibit 4 of John Pasquales and can confirm the following:

a. Pasquale's deposition Exhibit 3 (paras 7-10) states that he received a PCAP from IPP related to the IP address of the Defendant; that he used a commercial tool called Wireshark to verify the IP address and the date/time contained in the PCAP; and that he determined from the IP address (associated with the Defendant) that the Internet Service Provider (ISP) was Comcast Cable.

b. Pasquale's deposition Exhibit 4 discloses that he uses a workflow application program called Jira to obtain PCAPs and declarations to/from co-worker (Paul). His verification task involves analyzing the PCAP, determining the associated ISP, recording the ISP, signing the declaration, and returning it using Jira. (pp25-28). The declarations are used to obtain subpoena's for the purpose of obtaining the identity (name, contact info. etc.) of the IP address of the subscriber (e.g. the Defendant) (pp33-36);

c. Pasquale confirmed that PCAP files do not contain any information suggesting they were provided (sent) by the IPP system (they came from "Paul" using Jira (pp37-38)). Pasquale uses a utility program to look up the name of the ISP. He rejects the declaration if the PCAP cannot be verified (pp42-45). He was not able to confirm that he received all the PCAPs related to the IP address of the purportedly infringing IP address recorded in the PCAP (p49) or other PCAPs listed in the complaint for this case (p53-54). He acknowledged that PCAPs contain non-routable IP addresses communicating with the IP address of the Defendant (pp72-74).

6. Patrick Paige Background and Expertise

I have reviewed declaration Exhibit 5 and expert report Exhibit 6 of Patrick Page.

Mr. Paige outlines his experience as a police officer, detective in a crimes unit, investigation of child pornography, subpoenas, and search warrants. He discloses some familiarity with using software programs to investigate computers, likely personal computers. His roles appear to be mostly supervisory. He provides little evidence of the level of experience he has with complex software-based systems such as IPP. He provides opinions about WiFi networks, password protection, and hacking in the absence of supportive facts or data. He does not appear to have any experience in systems or software engineering, software design, coding, testing, or quality assurance. His declaration and expert report describes simplistic tests he has setup and applied to the IPP system which I discuss further below.

7. Stephen Bunting Background and Expertise

I have reviewed declaration Exhibit 7 of Stephen Bunting.

Mr. Bunting outlines his considerable experience as a police officer, digital, network, and cyber forensics consultant, training, author, fact witness, and investigation of child sexual abuse. He discloses some familiarity using software programs to investigate computers. He does not appear to have any experience in systems or software engineering, software design, coding, testing, or quality assurance. He provides little evidence of the level of experience he has with complex software-based systems such as IPP. He describes some aspects of the Wyoming Toolkit without providing details about the level of hands-on experience with the tool. He also describes tests he conducted for MaverickEye on a system that is similar to IPP. I comment about the tests he describes below.

8. Tests Conducted by Paige and Bunting

Having reviewed declaration Exhibit 5 and expert report Exhibit 6 of Patrick Page, and the declaration of Stephen Bunting, I can confirm the following.

The tests described by Paige and Bunting are trivial tests that set up three or four test computers with installed BitTorrent clients connected to Internet service providers configured to share a small number (e.g. 4) predetermined video files using BitTorrent. These simplistic "demonstration tests" confirm that all the pieces of the videos were detected and captured by IPP. However, the IPP system's operating workload at the time of the tests, and the workload conditions in the BitTorrent swarm were not described. And their tests did not document the operating workloads or churn among peers participating in the BitTorrent swarm during the period of the testing.

Paige and Bunting's tests demonstrate nothing about the reliability of the IPP software when operated under real-world operating conditions. They have not attempted to address the problems associated with routers using dynamic IP addressing (i.e. IP address resets), or conduct tests that attempt to determine if more than one user is attached to the router, or that the user has aborted an unintended download, or that a user has shut down because all the pieces of a movie have been received from other users in the swarm.

At the very least, these tests should have simulated router resets by powering them down and rebooting them during file sharing, and by running scenarios where BitTorrent users abort the downloading of shared video files before completion. Such operationally representative tests would have confirmed whether the IPP software could cope with unusual circumstances and events, and whether all the pieces of a video file could be received by users collaborating across an intensively active BitTorrent swarm.

9. Testing Conducted by Paige and Bunting as it Relates to Stalzer and Pasquale

9.1 Concerns Relating to Stalzer's Declaration and Deposition

Now relating Stalzer Exhibits 1 and 2 to testing conducted by Paige and Bunting, I can confirm:

a. None of the tests conducted by Paige or Bunting verified that "infringing files" (movies) were reliably transferred from the IPP system to the verification tool to support Stalzer's verification work;

b. Neither Paige nor Bunting conducted tests that the entirety of an "infringing file" associated with the IP address of a purported infringing user was transferred to the verification tool, that is, that an entire movie verified by Stalzer were indeed determined to have been captured from the purported infringer;

c. No tests were performed to verify that the *control copies* retrieved from the torrent website(s) used by Stalzer are actually owned by Strike 3, for example, by checking file hashes;

d. No tests were performed to verify that the "infringing file" and the control copy retrieved from the torrent website are computationally identical – this could be done by calculating and comparing file hashes;

Facts of the Matter: In the absence of successfully executed tests a., b., c. and d. above, the Plaintiff's experts (Paige and Bunting) have <u>not demonstrated</u> the following facts:

i. that infringing files were reliably transferred to the verification tool from IPP;

ii. that the entire file received by the verification tool was received from a single infringing user;

iii. that the control copy used by the verification tool was actually owned by Strike 3.

Given these facts, IPP may well have been routinely delivering false positive reports to Stalzer.

Additional Findings: Brandon Garcia-Paeth (Exhibit 8) and Kal Toth (Exhibit 9) confirm that in the present case, IPP downloaded at most 2 pieces (0.007%) of each of the purportedly infringed files from the Defendant's IP address. This raises several serious questions:

#1 By way of the verification tool, how could Stalzer have successfully played the "infringed file" delivered by IPP given that IPP reported detecting only a tiny fraction (0.007%) of the file?

#2 Could it be that IPP actually delivers an infringed file collected from many BitTorrent users?

#3 Could it be that IPP actually delivers a playable copy that is not acquired by way of BitTorrent?

These findings additionally undermine assertions by IPP's experts that IPP is a reliable forensics tool.

9.2 Concerns Relating to Pasquale's Declaration and Deposition

Now relating Pasquale Exhibits 3 and 4 to testing conducted by Paige and Bunting, I can confirm:

a. None of the tests conducted by Paige or Bunting verified that the PCAPs and declarations provided to Pasquale were reliably transferred to him from IPP by way of the Jira tool.

b. Neither Paige nor Bunting's tests verify how many PCAPs have been collected from a purported infringer and delivered to the PCAP verifier.

Facts of the Matter: In the absence of successfully executed tests a. and b. above, the Plaintiff's experts (Paige and Bunting) have <u>not demonstrated</u> the following facts:

i. that PCAP files and declarations are reliably transferred from IPP to Pasquale over Jira for PCAP verification, ISP lookup, signature, and submission back to Paul;

ii. that all the PCAPs necessary to assemble a complete/playable movie were received, verified (PCAP and ISP), signed, and submitted to IPP (via Jira and Paul).

Given these facts, Pasquale could be routinely receiving faulty PCAP files and declarations.

Additional Findings: Brandon Garcia-Paeth (Exhibit 8) and Kal Toth (Exhibit 9) confirm that in the case of the Defendant, IPP downloaded at most 2 pieces (0.007%) of each of the purported 80 to 87 files alleged to have been infringed. This raises the following concern about IPP's business model:

> *Stalzer's task attempts to verify that an infringed movie file can be viewed in its entirety, and compared to a control copy, prior to Stalzer signing a declaration that asserts infringement.*
>
> *In stark contrast, Pasquale's task verifies PCAPs collected from purportedly infringing BitTorrent users. The verifier completes, signs, and submits a declaration in preparation for a possible request to issue a subpoena, and action that is launched immediately upon receiving the first PCAP of a movie from IPP.*

These verification efforts of Stalzer and Pasquale appear to be at odds with each other.

My rate is $350.00 per hour.

K.C. Toth.

Signed under the Penalty of Perjury,
Kal Toth (Kalman C. Toth), Ph.D., P.Eng.

Exhibit 1

Declaration of Susan B. Stalzer in Support of Plaintiff's Motion for Leave to Serve a Third Party Subpoena Prior to Rule 26(f) Conference, Case No.: 2:17-cv-01731-MJP, Document 4-5, filed 11/29/17.

The Honorable Marsha J. Pechman

UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF WASHINGTON

AT SEATTLE

STRIKE 3 HOLDINGS, LLC, a Delaware corporation, Plaintiff, vs. JOHN DOE subscriber assigned IP address 73.225.38.130, Defendant.	Case No.: 2:17-cv-01731-MJP **DECLARATION OF SUSAN B. STALZER IN SUPPORT OF PLAINTIFF'S MOTION FOR LEAVE TO SERVE A THIRD PARTY SUBPOENA PRIOR TO A RULE 26(f) CONFERENCE**

[Remainder of page intentionally left blank]

EXHIBIT D

DECLARATION OF SUSAN B. STALZER IN SUPPORT OF PLAINTIFF'S MOTION FOR LEAVE TO SERVE A THIRD PARTY SUBPOENA PRIOR TO A RULE 26(f) CONFERENCE

I, Susan B. Stalzer, do hereby state and declare as follows:

1. My name is Susan B. Stalzer. I am over the age of 18 and am otherwise competent to make this declaration.

2. This declaration is based on my personal knowledge and, if called upon to do so, I will testify that the facts stated herein are true and accurate.

3. I work for Strike 3 Holdings, LLC ("Strike 3") and review the content of their motion pictures.

4. I hold a Bachelor's degree and Master's degree in English from Oakland University.

5. I have a long history of working in the fine arts, with an emphasis on writing, including having served as an adjunct professor of composition and literature.

6. I am familiar with Strike 3's plight with online piracy and its determination to protect its copyrights.

7. I was tasked by Strike 3 with verifying that each infringing file identified as a motion picture owned by Strike 3 on torrent websites was in fact, either identical, strikingly similar or substantially similar to a motion picture in which Strike 3 owns a copyright.

8. IPP provided me with the infringing motion picture file for each of the file hashes listed on Exhibit A to Strike 3's Complaint.

9. I viewed each of the unauthorized motion pictures corresponding to the file hashes side by side with Strike 3's motion pictures, as published on the *Blacked, Tushy* and/or *Vixen* websites and enumerated on Exhibit A by their United States Copyright Office identification numbers.

10. Each digital media file, as identified by the file hash value, is a copy of Strike 3's corresponding motion picture and is identical, strikingly similar or substantially similar to the

EXHIBIT D

original work identified by their United States Copyright Office identification numbers on Exhibit A to the Complaint.

DECLARATION

PURSUANT TO 28 U.S.C. § 1746, I hereby declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 20th day of November, 2017.

SUSAN B. STALZER

By:____________________

EXHIBIT D

Exhibit 2

Extracted pages from the rough transcript of the deposition of Susan B. Stalzer deposition, 4/16/19, pp. 29, 33, 49, 58, 75, 76,118, 133, 138, 140, 141

THIS IS AN UNCERTIFIED ROUGH DRAFT
AND CANNOT BE QUOTED IN ANY PLEADINGS
OR USED FOR ANY PURPOSE OTHER THAN
CASE PREPARATION AND MAY NOT BE
FILED WITH ANY COURT

This uncertified rough draft has not been proofread and may contain untranslated stenographic symbols, an occasional reporter's note, a misspelled proper name and/or nonsensical word combinations. All such entries will be corrected on the final certified transcript.

Due to the need to correct entries prior to certification, you agree to use this draft only for the purpose of augmenting counsel's notes and not to use or cite it in any court proceeding.

Please keep in mind that the final certified transcript page and line numbers will not match the rough draft due to the not clear to me.

Q. Okay. Well, let's walk through it.

First day you got this job at -- for Strike 3 Holdings, how did you verify the first work?

A. We have a verification tool in which I can play the clips.

Q. Okay. What is the name of that verification tool?

A. Verification tool.

Q. Okay. Who made the verification tool?

A. I have no idea.

Q. How do you know the verification tool works?

MR. BANDLOW: Objection. Vague and ambiguous.

THE WITNESS: It works in what regard? I don't understand the question.

and you open up the verification system.

A. Correct.

Q. What's the first thing you see when you open up the verification system?

A. A list of hash marks. A list of the site that the film is purported to be coming from, the title that is believed to be attached to this film and a button where I can hit play for the film to pop up for me to view it.

Q. Okay. And how is that information organized?

MR. BANDLOW: Objection. Vague and ambiguous.

THE WITNESS: Often alphabetically by title.

BY MR. EDMONDSON:

Q. Okay. Is it organized by case?

A. No, sir.

(Whereupon, the record was read.)

THE WITNESS: It's my understanding that the productions that they put out, they own copyrights on.

BY MR. EDMONDSON:

Q. How is that your understanding?

A. Because they are branded as their material. I guess I'm not sure how to answer that more clearly.

Q. Okay. So you have seen a number of the Strike 3 Holdings movies?

A. I have.

Q. Okay. And where on the movies does it say Strike 3 Holdings?

A. Okay. Fair enough. I know they're owned by the sites. The connection between the websites where the movies are put forth for membership in viewing versus Strike 3's relationship with that copyright, I have no knowledge.

Q. Okay. So you talked about the websites. Did you ever see the words have enter a user ID and password?

A. Yes.

Q. And what is that user ID and password?

MR. BANDLOW: That's confidential.

MR. EDMONDSON: We can mark it as confidential.

THE WITNESS: It's independent to me.

BY MR. EDMONDSON:

Q. I'm not asking what it's independent to. I'm asking what your user ID and password is.

MR. BANDLOW: We're not going to give that. I'll instruct the witness not to answer. It's her user ID and password. So we're not going to give that to you.

MR. EDMONDSON: There's nothing privileged about the user ID and password.

MR. BANDLOW: I'm still not going to give that to you based on your history with harassing her, so, no, you're not getting it. So next question.

MR. EDMONDSON: It's not her property, it's the property of Strike 3 Holdings.

MR. BANDLOW: I understand, but I'm

marked Page 3. Have you ever described yourself as a comparer?

A. I think it's a fair description.

Q. Okay. But did you talk to anybody -- well, have you ever seen this text here before?

A. I did not.

Q. You did not draft this information here?

A. No, sir.

Q. So you didn't tell someone at Fox Rothschild that you're a comparer?

A. No.

MR. BANDLOW: We came up with that lovely word, Curt. We're very proud of it.

BY MR. EDMONDSON:

Q. And you see here, possesses information that the motion pictures identified by their cryptographic hash value on the BitTorrent network that defendant's IP address infringed correspond to motion pictures owned by Strike 3.

Now, we just looked at Document 62 there, correct --

A. Correct.

Q. -- the screen of the verification system?

Is there an IP address anywhere on that screen?

A. Not that I have, no.

Q. And do you know of any IP addresses in this case?

A. No.

Q. Do you know of any IP addresses in any case?

A. No.

Q. Do you know your own IP address?

A. Not offhand, no.

Q. Let me hand you a document marked Exhibit 45. Miss Stalzer, have you seen this document before?

A. No.

Q. Have you ever seen a complaint in any

Conference?

A. Yes, I see that.

Q. So when -- did you, when you signed this declaration, did you read that caption?

A. I'm not given the cover pages when the declarations are sent to me.

Q. I see. So you don't know if it's for a particular case, correct?

A. I don't have the case number that's attached.

Q. Okay. How many declarations have you signed?

A. I don't know exactly.

Q. Well --

A. From your own information, it seems to be over 3,000.

Q. Does that seem right?

A. Yes, sir.

Q. From Oakland University?

A. Yes.

Q. Would you say your command of the English language is probably better than the average person's?

MR. BANDLOW: Objection. Calls for speculation. Vague and ambiguous.

Go ahead and answer.

THE WITNESS: I don't know that I'm arrogant enough to put myself above and beyond other people. I feel I have a reasonable command of the English language.

BY MR. EDMONDSON:

Q. Okay. Now, the sentence IPP provided me with the infringing motion picture file, did IPP provide you with the infringing motion picture file?

A. Through the verification tool, yes.

Q. But that's not what that says. It doesn't say IPP provided me with the infringing motion picture file through the verification

A. Again, it would vary depending on the situation. There have been times more often than direct communication between Tobias and myself, Sud will communicate with me and copy Tobias or communicate with Tobias and copy me, "When is the next batch being uploaded," something to that effect.

Q. And what's Tobias's e-mail address?

A. I don't know off the top of my head.

Q. But IPP did not provide you with the infringing motion picture, the verification system provides you with that?

A. They have to get there somehow. They have to get into the verification tool some way, and IPP is the way in which they are loaded into the verification tool.

Q. But there's nothing on the verification tool that says IPP on it, correct?

A. Not to my knowledge.

Q. Okay. Now, looking at Paragraph 9 of this declaration, do you see reference to Exhibit A?

A. Yes.

for me.

BY MR. EDMONDSON:

Q. Now, going back to Exhibit 62 [Sic], and you see Paragraph 10 on your declaration, how do you note whether the motion picture and the digital media file is identically identical or strikingly similar or substantially similar?

A. Through the number of different ways I use to verify, as I had stated earlier.

Q. Yeah, but those are three different categories. So do you have a notation system of determining which of these works were identical, which were strikingly similar and which were substantially similar?

A. No.

Q. How do you distinguish between those three characteristics?

A. I do not have a measure with which to grade between those three categories. I guess the only way I know how to answer that question is that before I will verify something is good, that I am confident that they are the same film.

Q. Okay. But you used three words in this declaration.

A. The declaration states three different ways.

Q. The declaration states three different characteristics, or three different analysis, identical, strikingly similar or substantially similar.

What I'm asking is how do you characterize each of those three species?

MR. BANDLOW: Objection. Asked and answered.

Try again.

THE WITNESS: I don't particularly

Exhibit 3

Declaration of John S. Pasquale in Support of Plaintiff's Motion for Leave to Serve a Third Party Subpoena Prior to Rule 26(f) Conference, Case No.2:17-cv-01731-MJP, Document 4-4, filed 11/29/17

The Honorable Marsha J. Pechman

UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF WASHINGTON

AT SEATTLE

STRIKE 3 HOLDINGS, LLC, a Delaware corporation,

Plaintiff,

vs.

JOHN DOE subscriber assigned IP address 73.225.38.130,

Defendant.

Case No.: 2:17-cv-01731-MJP

DECLARATION OF JOHN S. PASQUALE IN SUPPORT OF PLAINTIFF'S MOTION FOR LEAVE TO SERVE A THIRD PARTY SUBPOENA PRIOR TO A RULE 26(f) CONFERENCE

[Remainder of page intentionally left blank]

EXHIBIT C

DECLARATION OF JOHN S. PASQUALE IN SUPPORT OF PLAINTIFF'S MOTION FOR LEAVE TO SERVE A THIRD PARTY SUBPOENA PRIOR TO A RULE 26(f) CONFERENCE

I, John S. Pasquale, do hereby state and declare as follows:

1. My name is John S. Pasquale. I am over the age of 18 and I am otherwise competent to make this declaration.

2. This declaration is based on my personal knowledge and, if called upon to do so, I will testify that the facts stated herein are true and accurate.

3. I am a Senior Project Manager with 7 River Systems, LLC a Maryland based cyber security firm specializing in network security, data breaches, and the protection of secured information transmitted across networks.

4. For over 30 years, I have worked in the IT industry, specializing in system and network administration and project management.

5. I have consulted and advised major financial institutions and Fortune 500 companies on the management, security and implementation of major data centers, delivering complex and large scale network projects.

6. I was retained by Strike 3 Holdings, LLC ("Strike 3") to individually analyze and retain forensic evidence captured by IPP International U.G. ("IPP").

7. I received a PCAP from IPP containing information relating to the transaction occurring on 09/05/2017 10:40:33 involving IP address 73.225.38.130.

8. I used a program called Wireshark to view the contents of the PCAP.

9. I was able to confirm that IPP recorded the transaction with 73.225.38.130 at 09/05/2017 10:40:33.

10. Based on my experience in similar cases, Defendant's ISP Comcast Cable is the only entity that can correlate the IP address to its subscriber and identify Defendant as the person assigned the IP address 73.225.38.130 during the time of the alleged infringement. Indeed, a subpoena to an ISP is consistently used by civil plaintiffs and law enforcement to identify a subscriber of an IP address.

DECLARATION

PURSUANT TO 28 U.S.C. § 1746, I hereby declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 24th day of November, 2017.

JOHN S. PASQUALE

By:

Exhibit 4

Extracted pages from the rough transcript of the deposition on John S. Pasquale, 04/17/19, pp. 25-28, 33-36, 37-38, 42-45, 53-54, 72-74

(INSERT CAPTION/APPEARANCES/INDEX/SWORN)

STARTTIME9:40AM 4/17/19

(EXHIBIT MARKED/70)

Q Good morning, Mr. Pasquale.

A Good morning.

Q Could you please state and spell your name for the record?

A John Pasquale, J-o-h-n, P-a-s-q-u-a-l-e.

Q Do you have a middle name?

A Yes, Santo, S-a-n-t-o.

Q Excellent. Mr. Pasquale, have you ever been deposed before?

A No, I have not.

Q Some of the grounds rules for a deposition is the Court Reporter is taking down our words, so if you can answer verbally, that would be appreciated. She can't record gestures.

A Understood.

Q If you nod yes or shake no, she can't take that down.

A Understood.

Q Do everything verbally. The other thing, too, is that I might ask you to either to estimate some things, so what I'd like to you do

Q Do you know the IP address for your router?

A No.

Q Do you ever analyze any of these PCAPs on a laptop?

A No.

Q So you keep everything on your computer?

A Yes.

Q While you're doing this PCAP analysis, are you making any notes of your analysis?

A No.

Q When you're done analyzing the PCAP, what do you do with it?

A I upload it to a program called JIRA, which is a workflow application and send them off to Paul for review.

Q JIRA?

A J-I-R-A.

Q The PCAP comes in from -- is it Paul?

A Yes.

Q Is that attached to an email?

A No, it's through JIRA.

Q So you have a JIRA application. Who is on the JIRA application?

A I'm not sure I understand the question.

Q Explain JIRA to me.

A So JIRA is a workflow application. In this case PCAPs and declarations are attached to a particular case. Then from there I pull up those two documents and analyze, sign and save.

Q You get the declaration and the PCAP. Are they both together in the same --

A They're together in the same case, yes.

Q Just so the record is clear, when we use the word "case," in the legal profession we're usually referring to something like a lawsuit. When you're using the word "case," what do you mean?

A When I'm using the word "case," it is one declaration and one PCAP.

Q In the JIRA?

A Yes.

Q Is there any notation that says this is for a lawsuit number, and in this case 2:17-cv-01731?

A There are numbers attached to it. I'm not sure if they coincide with a lawsuit.

Q When is the last time you looked at the JIRA app?

A Three days ago.

Q Describe what you saw in that last transaction?

A So the case, what I'm calling the case would have a number associated with it, an abbreviation of a district, what state that it's in, and then the actual district within the state, and I believe that's it.

Q Is the number a four-digit number?

A Yes. I believe so, yes.

Q Then when you get it in on JIRA, do you save the PCAP to your desktop?

A Yes.

Q Do you save the declaration to the desktop?

A Yes, on a temporary basis. I don't save the PCAP. I save the declaration.

Q You put the declaration on your desktop?

A I save it locally, and then I upload it, and then once I'm done, I delete it from my desktop.

Q Were you ever given instructions by Paul not to delete data?

A No.

Q Were you ever given instructions by Paul to organize the data that you analyze on your system in some directories or folders by the four-digit case number?

A In my system, no.

Q So Paul never said to you to keep a record of the analysis that you have done in these cases. Is that correct?

A No. The records are stored on JIRA. That's what JIRA is for.

Q I understand, but my question was, did he ask you to keep a local independent record of the analysis that you did?

A No.

Q So as we speak right now, the only record that you have of your analysis would be the transactions and JIRA?

A Correct.

Q And obviously the declarations filed in the courts. Correct?

A Say that again.

Holdings, LLC produced on the internet, via the internet?

A Before I signed any declaration, it was explained to me by Paul exactly what Strike 3 is. In fact, he consulted with me on whether or not to take on the client, and that was our conversation about Strike 3 and what they do.

Q Did Paul tell you not to do any independent research into Strike 3 Holdings?

A No.

Q So you didn't have the natural curiosity to go out and google "Strike 3 Holdings"?

A I'm a very busy man.

Q But you've signed hundreds of declarations for Strike 3 Holdings. True?

A Yes.

Q Let's go to the next line. Do you see line 26 there? Do you see that phrase, "Indeed, a subpoena to an ISP is consistently used by civil plaintiffs and law enforcement to identify a subscriber of an IP address."

What is your experience with subpoenas?

A None.

Q Why did you use that word in there?

A Well, to me a subpoena is a document through the courts to go to an ISP and obtain an IP address and who that IP address belongs to.

Q The statement is, "Indeed, a subpoena to an I SP is consistently used by civil plaintiffs and law enforcement to identify a subscriber of an IP address."

What experience do you have that supports that statement that you made there?

A I know that you would need some type of court order to obtain an IP address.

Q How do you know that?

A Through my experience in the IT industry.

Q What experience has that been?

A It's 35 years of experience.

Q Have you ever worked for an attorney on a subpoena to an ISP?

A No, I have not.

Q Have you ever actually drafted a subpoena going to an ISP?

A No, I have not.

Q What engagements did you ever deal with subpoenas going to ISP's?

A None.

Q So I want to -- when you say the word there "indeed, a subpoena," that suggests to me a very clear affirmative statement that you've done this a lot, but my understanding is you've never participated in sending subpoenas to an ISP. Is that correct?

A I have not. You're probably misinterpreting that line.

Q I want to know why you wrote it.

A I wrote it because it's my understanding that a subpoena is needed to go to a -- a court order is needed in order to get an actual person attached to an IP address, through the ISP.

Q Did you draft this sentence? Did you sit down at a computer --

A No, I did not.

Q Who drafted this sentence?

A This was given to me by 7 Rivers.

Q Do you know if Paul drafted this sentence?

A I don't know.

Q I want you to turn to the next page please. Do you see the declaration there at the top?

A Yes.

Q And do you see there, "Pursuant to 28 U.S.C. 1746"?

A Uh-huh.

Q What's your understanding of the next sentence, "I hereby declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct"?

A That anything that I'm saying here -- that anything that is said in this document that I'm signing, that it's true and correct.

Q How do you know this is true and correct?

A I know it's true and correct by the PCAP that I reference.

Q I mean, going back to Line 26 and 27. From experience?

A From experience.

Q But you didn't draft that statement?

A No, I did not.

Q And you testified earlier that you've never had experience sending subpoenas to ISPs?

A That's correct.

Q You testified earlier -- and I want to make sure. In Paragraph 7 of your declaration you said, "I received a PCAP from IPP," but I understood you received a PCAP from Paul on JIRA.

A Correct.

Q So why doesn't that sentence say, "I received a PCAP from Paul on JIRA containing information relating to the transaction"?

A I would assume that 7 Rivers Systems is the handler, but the original document comes from IPP.

Q That's an assumption. Correct?

A Yeah, I guess so.

Q So Paragraph 7 did you -- you didn't draft Paragraph 7?

A As I said, I didn't draft this document. I reviewed the document. I look at the content of the document. I ensure that the content in the document is correct according to the PCAP, and then from there sign it.

Q What I'm trying to do is find out if there's any inaccuracies in this document so, in Paragraph 7 you didn't receive a PCAP from IPP. You received the PCAP from Paul using the JIRA system. Correct?

A Sure, you can say that, but the document originates from IPP and Strike 3 Holdings.

Q How do you know that?

A Because Strike 3 Holdings is the client of 7 Rivers Systems.

Q Do you do computer forensics?

A Actually, that's what this is.

Q And so you're familiar with concepts of chain of custody?

A Sure.

Q Did you verify the chain of custody of this data coming from IPP to 7 Rivers Systems to your JIRA and then to your desktop? Did you verify every step?

A No, I did not.

(EXHIBIT MARKED/73)

Q I'm going to hand you a blank sheet marked 73. Can you sketch out the system architecture of the IPP monitoring system to the best of your knowledge?

A I cannot.

Q Can you describe then for me in your best understanding what the IPP system does?

A No.

Q Do you know where it's located?

A I believe they're in Germany, but I'm not a hundred percent sure.

Q Did you ever ask to visit the IPP facility?

A No.

Q Did you ever ask to speak to anybody at IPP?

A No.

Q Why not?

A It's not part of my job description. It's above my pay grade.

Q Do you know that these declarations have been used in lawsuits?

A Yes.

Q Have you ever been sued?

A No.

Q What data inside the PCAP would suggest to you that it came from IPP?

A What data?

Q Right.

A None.

Q There's nothing in the PCAP that it came from IPP?

A I don't believe so.

Q In your analysis -- going to Paragraph 10, do see Line 23 there on the declaration we've marked as Exhibit 71?

A Uh-huh.

Q "Based on high experience in similar cases."

What other similar cases were you referring to when you said that?

A Other cases that have PCAPs and use Comcast as the ISP.

Q Well, defendant's ISP, Comcast Cable, how did you know it was Comcast?

A There's a program that you can run the IP address, and it will tell you exactly who the ISP is.

Q Did you run that program?

A Yes, I did. For this one I believe I did, yes.

Q What's the program?

A I don't have it off the top of my head, but I can certainly send it to you if you like. You can look it up and google it, and probably 4,000 will come up.

Q When you did this analysis you

looked at JIRA. Right? You got the PCAP and the declaration from JIRA?

A Correct.

Q And you also took and copied -- and correct me if I'm wrong. You copied the IP address into this other program to look up who the cable provider is. Correct?

A Who the ISP is.

Q And then what did you do? A screen print of that?

A No.

Q How did you confirm that that was Comcast?

A I confirmed what was in the documents stating that the defendant's ISP was Comcast because it was already written there. As I said, I did not draft these documents. I'm verifying the documents.

Q You verified it using a program, but you didn't keep a record of your verification?

A No, I did not.

Q Did you have like a?

A This is the record of my verification.

Q Did you have a notebook or

spreadsheet that would say --

A No.

Q What happened if you got -- if it didn't verify? What would you do?

A I would reject the declaration.

Q How many of these declarations have you rejected?

A At first there was quite a few. I can't give you an exact amount, but at first I would say ten percent, maybe more. I don't know. I don't recall.

Q Did you make notes in JIRA --

A Yes.

Q -- on those rejections?

A Yes, I did.

Q So when you saw rejections, did you ask Paul -- is that your son?

A Uh-huh.

Q Did you ask Paul, Why are we getting these rejections?

A Only if it was at a high rate, and there was one point where there was a high rate, but it wasn't due to the wrong ISP. It was more toward the time stamp itself.

(EXHIBIT MARKED/45)

A I would surmise that it would be Paul if he did.

Q It's a small company.

A Yes.

Q It's a family-run company.

A I don't know if it's family run, but it's run by my son.

Q Before I became a lawyer, I was in the software business with my dad, so I'm familiar with the setup.

Now that you know that 80 works were alleged to have been infringed --

A I know that because you just told me, but go ahead.

Q This is a Complaint filed by your customer, strike 3 Holdings, something your customer drafted, not me. Now that you know that 80 works were alleged to have been infringed and now that you've established your professional and cyber investigations --

A You can label it that.

Q If I labeled it incorrectly, please let me know.

A That's fine.

Q Would you have requested PCAPs on

these other 79 works?

A If I would have known that they were all interconnected? I don't know to be honest. I would just be -- I would ask for counsel's guidance.

Q Would you consider your investigation to be thorough if you only looked at one out of 80 PCAPs?

A Yes.

Q Let's explore that. Do you see under the UTC column where it says 9/5/2017?

A Yes.

Q And you testified earlier and you filed a declaration saying you know something about Comcast Cable. Correct?

A Uh-huh.

Q And do you know if this IP address supplied by Comcast Cable was static or dynamic?

A Don't know.

Q Do you understand the difference between a static and dynamic IP address?

A Yes.

Q Explain to me the different between a static and a dynamic IP address.

A A static IP address is one that's

A No, I did not.

Q You didn't look up the source IP address?

A No.

Q Is there anything about that source IP address that is unusual?

MR. ATKIN: Objection to form. You can answer if you understand.

A No.

Q You're familiar with the internet topology?

A Yes.

Q Are you familiar with nonroutable IP addresses?

A Nonroutable IP addresses? To a certain extent.

Q I probably slurred my words. Nonroutable IP address?

A Okay.

Q When you studied internet topology, were you aware of blocks of IP addresses that are designated as not allocated to a particular computer?

A I'm not sure I understand your question.

Q You understand in the network architecture of the internet that every computer is assigned an IP address?

A Correct.

Q And since there's billions of computers, there's not enough IP addresses to go around. Correct?

A Yes.

Q And so the way the internet has been organized is that behind routers they will have internal IP?

A Nonregistered IP addresses.

Q And then for everybody to communicate across the internet, you have actual IP addresses?

A Correct.

Q And there's blocks of IP addresses that have been designated that won't route to the outside internet?

A Correct.

Q Otherwise everything would be blow up?

A It would be mayhem, yes.

Q Do you know what those blocks of nonroutable IP addresses are?

A No.

Q If that IP address turns out to be nonroutable, would it have changed your analysis and your declaration?

MR. ATKIN: Objection. What is that IP address?

Q Let's put it on the record now that you brought that up. Can you read off the IP address of Line 2 there?

MR. EDMONDSON: If you can confirm it counsel because I'm not looking it?

A 192.168.0.13.

MR. ATKIN: He asked for Line 2.

THE WITNESS: This is Line 2, destination.

Q In this transactions, there's two IP addresses. Correct?

A Uh-huh.

Q Because we have this computer communicating with --

A Yes.

Q So in this transaction we don't see three or four IP addresses. It's just --

A Per transaction within the PCAP.

MR. EDMONDSON: Off the record

Exhibit 5

Declaration of Patrick Paige, S3H (217-cv-01731)_000166, filed 11/12/13

DECLARATION OF PATRICK PAIGE

I, PATRICK PAIGE, DO HEREBY DECLARE:

1. I am over the age of eighteen (18) and otherwise competent to make this declaration. The facts stated in this declaration are based upon my personal knowledge.

2. I was a police officer from 1989 until 2011 for the Palm Beach County Sherriff's Department. And, from 2000-2011, I was a detective in the computer crimes unit.

3. As a detective in the computer crimes unit, I investigated internet child pornography and computer crime cases.

4. I have conducted forensic computer examinations for:

(a) Broward County Sheriff's Office (BSO);

(b) Federal Bureau of Investigation (FBI);

(c) U.S. Customs and Border Protection (CBP);

(d) Florida Department of Law Enforcement (FDLE);

(e) U.S. Secret Service;

(f) Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); and

(g) Various municipalities in the jurisdiction of Palm Beach County.

5. I was also previously assigned to a police unit working in conjunction with TLO Corp., which is a private company.

6. When I worked with TLO Corp., I supervised the other detectives assigned to the unit, which was consisted of six online investigators and two computer forensic examiners.

7. I am familiar with software programs used to investigate computers, including EnCase and Access Data.

8. I have taken over 400 hours of courses designed to teach people how to investigate computers.

9. Also, while working from 2003-2011 for Guidance Software, the makers of EnCase, I have taught over 375 hours of courses in computer forensics ranging from beginner to advanced levels.

10. I have had students in my courses from various government branches, including: (a) sheriff's offices; (b) FBI agents; (c) ATF agents; (d) agents from the Central Intelligence Agency, and (e) individuals from other branches of government and the private sector.

11. After leaving the Palm Beach County Sherriff's office, I founded Computer Forensics, LLC, where I am currently employed.

12. I have received the following awards and commendations:

(a) 1991 – Deputy of the Year, awarded by the 100 Men's Club of Boca Raton & Rotary Club.

(b) 1997 – Deputy of the Month for June.

(c) 2001 – Detective of the Month for October.

(d) 2002 – Outstanding Law Enforcement Officer of the Year, awarded by the United States Justice Department for work in the *U.S. vs. Jerrold Levy* case.

(e) 2003 – U.S. Customs Service Unit Commendation Citation Award for computer forensic work in Operation Hamlet. Operation Hamlet was one of the largest rings in the history of U.S. Customs of individuals who were molesting their own children, and transmitting the images and video via the Internet.

(f) 2005 – Detective of the Month for December.

(g) 2007 – Outstanding Law Enforcement Officer of the Year, awarded by the United States Justice Department for work in the *U.S. vs. Jimmy Oliver* case.

(h) 2008 – Letter of Commendation issued by the FBI for outstanding computer forensic work in the *U.S. vs. Frank Grasso* case.

13. I have been called to testify as a fact and expert witness on numerous occasions in the field of computer forensics in both trial-level and appellate proceedings before state, federal, and military courts in Florida, California, New Jersey, and New York.

14. No court has ever refused to accept my testimony on the basis that I was not an expert in computer forensics. My skill set and my reputation are my most important assets in my current position with Computer Forensics, LLC.

15. With regard to my experience investigating child pornography cases, I supervised police officers whose responsibility it was to establish a successful TCP/IP connection with persons who were sending pornographic images of children or other illegal content over the Internet.

16. The offenders' IP addresses, as well as the dates and times of the illegal transmission were recorded.

17. An officer would then request that the assistant state attorney subpoena the corresponding ISPs for the purpose of identifying the subscribers that were transmitting the illegal content.

18. In these cases, the subscribers were not notified by the ISPs that their identity was being subpoenaed because they could have deleted the images and destroyed the data.

19. After receiving the subscribers' identities, we would prepare a search warrant that would authorize us to enter the subscribers' dwelling and seize all of their computer devices.

20. I was directly involved in approximately 200 search warrants either by way of managing the process or performing it personally.

21. I can recall only one instance in all the times that we executed a search warrant and seized computers where we did not find the illegal content at the dwelling identified in the search warrant.

22. In that one instance, the Wi-Fi connection was not password protected, and the offender was a neighbor behind the residence.

23. I never came across a Wi-Fi hacker situation.

24. In my opinion, a child pornographer has a greater incentive to hack someone's Wi-Fi connection than a BitTorrent user because transmission of child pornography is a very serious crime with heavy criminal penalties, and many offenders can face life sentences if convicted.

25. I tested IPP International U.G.'s ("IPP") IP detection process.

26. To do so, I downloaded four public domain movies from the national archive.

27. I then encoded text into the videos, so that I would know whether someone that downloaded that particular movie downloaded the version of the movie that I created.

28. I then rented four virtual servers, each of which was connected to the Internet and used a unique IP addresses.

29. I then configured the servers so that all of them were running Windows 2008 server edition, and I put a different BitTorrent client onto each server.

30. A BitTorrent "client" is software that enables the BitTorrent protocol to work.

31. After installing the BitTorrent clients, I also installed Wireshark onto each server. "Wireshark" is a program that captures network traffic and creates PCAPs, just as TCP Dump, which IPP uses, does. A PCAP is like a video recording of all the incoming and outgoing transactions of a computer.

32. After installing Wireshark onto each of the servers, I transferred the movies from my local computer to the servers.

33. I then used the BitTorrent clients on each of the servers to make .torrent files. I uploaded these .torrent files onto various torrent websites.

34. I then informed IPP of the movie names. Thereafter, IPP sent me screen captures of the movies I had seeded.

35. The screen captures sent by IPP had my codes on them; thus, I knew that IPP had caught the movies I had seeded.

36. IPP also sent me additional data identifying the IP Address used by each of the four servers, and sent me PCAPs.

37. I reviewed IPP's PCAPs vis-à-vis the PCAP log files created by each of my test servers, and determined that IPP's PCAPs match my PCAPs. This could not have happened unless IPP's server was connected to the test server because the transactions would not match.

38. From this test, I concluded that IPP's software worked, and had a subpoena been issued for my IP addresses, it would have revealed my identity.

FURTHER DECLARANT SAYETH NAUGHT.

DECLARATION

PURSUANT TO 28 U.S.C. § 1746, I hereby declare under penalty of perjury that the foregoing is true and correct.

Executed on this 11th day of November, 2013.

By: Patrick Paige Digitally signed by Patrick Paige DN: cn=Patrick Paige, o=Computer Forensics LLC, ou, email=patrick@patrickpaige.com, c=US Date: 2013.11.11 15:53:41 -05'00'

PATRICK PAIGE

Honorable Thomas S. Zilly

UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF WASHINGTON

AT SEATTLE

STRIKE 3 HOLDINGS, LLC, a Delaware corporation, Plaintiff, vs. JOHN DOE subscriber assigned IP address 73.225.38.130, Defendant.	Case Number: 2:17-cv-01731-TSZ **REBUTTAL EXPERT REPORT TO STRIKE 3 HOLDING'S EXPERT REPORTS OF PAIGE AND BUNTING REGARDING RELIABILITY OF THE IPP INFRINGEMENT MONITORING SYSTEM**

Rebuttal Expert Report to Strike 3 Holding's Expert Reports of Paige and Bunting Regarding Reliability of the IPP Infringement Monitoring System

April 29th, 2019
Prepared by Dr. Kal Toth, P.Eng., Portland, OR 97205
For Mr. J. Curtis Edmondson, Law Offices of J. Curtis Edmondson, Hillsboro, OR 97124

In this report I rebut declarations and reports by the Plaintiff's experts (Paige and Bunting), relating their work to information disclosed by two members of IPP's operational staff. As indicated below I am of the opinion that the experts did not provide convincing facts, data, principles, methods, and reasoning demonstrating that the IPP system operates reliably for its intended purposes, namely to:

(a) detect and report infringement, and

(b) support the essential day-to-day procedures of verifying IPP system outputs by operational stafff.

The approach I have therefore taken is to first summarize the pertinent facts and data disclosed by way of the depositions of Stalzer and Pasquale, followed by discussions relating to the expertise and methods used by the Plaintiff's experts to test the operational IPP system.

Contents

1. My Approach

Below I describe operational scenarios highlighting pertinent facts, data and methods experts that Paige and Bunting have failed to address. These informational gaps imply there is a significant risk that IPP delivers an unacceptable number of false positive reports of infringement. By false positives I mean operational scenarios where data reported by the IPP system incorrectly binds an identifying attribute of a user, such as an IP address, with a copyrighted movie of the Plaintiff. More generally, I have defined:

> *false positives are undetected reports of infringement delivered to a plaintiff that could culminate in the issuance of a subpoena that wrongfully discloses the identity of an innocent party.*

Software and systems engineering professionals routinely apply best practices to ensure that the systems, software, and procedures they design and specify are reliable enough to minimize operational risks. To date, the Plaintiff's experts have not provided convincing facts and data showing that such best practices and have been applied to develop, test, quality assure, and maintain the IPP system. I understand that IPP is touted by some of IPP's experts to be a forensics tool that accurately identifies infringing BitTorrent users. I am of the opinion that IPP if cannot be relied upon to consistently discriminate between infringers and non-infringers, it should not be used for forensics purposes.

Should the Plaintiff's experts provide facts, data and method demonstrating that the system requirements are consistently satisfied by the operational system, I would gladly review and re-assess IPP's reliability (Exhibit 9).

I acknowledge that the false positive rates for complex systems are challenging to assess. I believe the burden of proof is on the owner of a forensics tool, such as IPP, to provide requisite facts, data, and methods that demonstrate that the system is sufficiently reliable to mitigate the risk of false positives being delivered.

2. Synopsis of My Qualifications

The opinions expressed in this report are drawn from my professional experience provided in the annex to my *Amended Expert Report: Reliability Assessment of IPP Software, Kal Toth, 04/15/19* (Exhibit 9). My most relevant qualifications include: independent validation and verification of a secure messaging network for Canada's embassies abroad; quality, reliability, maintainability, safety, security, and software engineering for Hughes Aircraft for Canada's air traffic control system; software engineering practice leader for CGI Group and Hughes Aircraft; and software engineering courses for ten universities including Portland State University, Oregon State University, and the Technical University of British Columbia (now part of Simon Fraser University).

3. Evidence Reviewed and Referenced

Exhibit 1 Declaration of Susan B. Stalzer in Support of Plaintiff's Motion for Leave to Serve a Third Party Subpoena Prior to Rule 26(f) Conference, Case No.: 2:17-cv-01731-MJP, Document 4-5, filed 11/29/17.

Exhibit 2 Extracted pages from the rough transcript of the deposition of Susan B. Stalzer deposition, 4/16/19, pp. 29, 33, 49, 58, 75, 76,118, 133, 138, 140, 141).

Exhibit 3 Declaration of John S. Pasquale in Support of Plaintiff's Motion for Leave to Serve a Third Party Subpoena Prior to Rule 26(f) Conference, Case No.2:17-cv-01731-MJP, Document 4-4, filed 11/29/17.

Exhibit 4 Extracted pages from the rough transcript of the deposition on John S. Pasquale, 04/17/19, pp25-28, 33-36, 37-38, 42-45, 53-54, 72-74.

Exhibit 5 Declaration of Patrick Paige, S3H (217-cv-01731)_000166, filed 11/12/13.

Exhibit 6 Expert Report Regarding Testing of IPP International UG's Infringement Detection System (Exhibit B), Patrick Paige Computer Forensics LLC, S3H (217-cv-01731)_000171, filed 11/06/18.

Exhibit 7 Declaration of Stephen M. Bunting, S3H (217-cv-01731)_000155, dated 12/11/18.

Exhibit 8 Declaration of Brandon Garcia-Paeth in Support of Defendant's Opposition to Plaintiff's Motion for Summary Judgment, Case no. 2:17-cv-01731-TSZ, 02/25/219.

Exhibit 9 Amended Expert Report: Reliability Assessment of IPP Software, Kal Toth, 04/15/19.

4. Video Verification, Susan Stalzer

Having reviewed declaration Exhibit 1 and deposition Exhibit 2 of Susan Stalzer, I can confirm the following:

a. Stalzer's declaration Exhibit 1 (paras 7 and 8) state that she was tasked to visually verify each *infringing file* provided to her by IPP to determine if it was identical to, strikingly similar to, or substantially similar to a motion picture (movie) identified as owned by Strike 3 on torrent websites;

b. Stalzer deposition Exhibit 2 discloses that she uses a *verification tool* to select and display from a list of movie titles on her computer screen, each having a hash mark, each representing a [purportedly] infringing file; and also displaying a copy of a movie owned by Strike 3 (control copy) obtained and displayed by logging into a torrent website, entering the same movie title into the search window of her browser, and downloading the file;

c. Stalzer in Exhibit 2 discloses that she uses the verification tool to select a file from the list, visually compares the two movies, and indicates whether they visually match ("good") or do not match ("bad") by pressing a button, recording failed matches ("bad") in an Excel spreadsheet. At some later date, she signs a declaration listing movies that she apparently identified as "good". With respect to her comparison task, Stalzer confirms (pp.140-141) that she does "not have a measure with which to grade between the three categories" [identical to, strikingly similar to, or substantially similar];

d. Apparently, Stalzer does not rely on the provided hashes to execute her task, and is not provided the IP address of purported infringer(s) via her verification tool. Her screen does not indicate that the infringed file was received from the IPP system or that the downloaded control copy of the movie is owned by Strike 3. The *verification tool* apparently interfaces with IPP and is not a commercial product;

5. PCAP Verification, John Pasquales

I reviewed declaration Exhibit 3 and deposition Exhibit 4 of John Pasquales and can confirm the following:

a. Pasquale's deposition Exhibit 3 (paras 7-10) states that he received a PCAP from IPP related to the IP address of the Defendant; that he used a commercial tool called Wireshark to verify the IP address and the date/time contained in the PCAP; and that he determined from the IP address (associated with the Defendant) that the Internet Service Provider (ISP) was Comcast Cable.

b. Pasquale's deposition Exhibit 4 discloses that he uses a workflow application program called Jira to obtain PCAPs and declarations to/from co-worker (Paul). His verification task involves analyzing the PCAP, determining the associated ISP, recording the ISP, signing the declaration, and returning it using Jira. (pp25-28). The declarations are used to obtain subpoena's for the purpose of obtaining the identity (name, contact info. etc.) of the IP address of the subscriber (e.g. the Defendant) (pp33-36);

c. Pasquale confirmed that PCAP files do not contain any information suggesting they were provided (sent) by the IPP system (they came from "Paul" using Jira (pp37-38)). Pasquale uses a utility program to look up the name of the ISP. He rejects the declaration if the PCAP cannot be verified (pp42-45). He was not able to confirm that he received all the PCAPs related to the IP address of the purportedly infringing IP address recorded in the PCAP (p49) or other PCAPs listed in the complaint for this case (p53-54). He acknowledged that PCAPs contain non-routable IP addresses communicating with the IP address of the Defendant (pp72-74).

6. Patrick Paige Background and Expertise

I have reviewed declaration Exhibit 5 and expert report Exhibit 6 of Patrick Page.

Mr. Paige outlines his experience as a police officer, detective in a crimes unit, investigation of child pornography, subpoenas, and search warrants. He discloses some familiarity with using software programs to investigate computers, likely personal computers. His roles appear to be mostly supervisory. He provides little evidence of the level of experience he has with complex software-based systems such as IPP. He provides opinions about WiFi networks, password protection, and hacking in the absence of supportive facts or data. He does not appear to have any experience in systems or software engineering, software design, coding, testing, or quality assurance. His declaration and expert report describes simplistic tests he has setup and applied to the IPP system which I discuss further below.

7. Stephen Bunting Background and Expertise

I have reviewed declaration Exhibit 7 of Stephen Bunting.

Mr. Bunting outlines his considerable experience as a police officer, digital, network, and cyber forensics consultant, training, author, fact witness, and investigation of child sexual abuse. He discloses some familiarity using software programs to investigate computers. He does not appear to have any experience in systems or software engineering, software design, coding, testing, or quality assurance. He provides little evidence of the level of experience he has with complex software-based systems such as IPP. He describes some aspects of the Wyoming Toolkit without providing details about the level of hands-on experience with the tool. He also describes tests he conducted for MaverickEye on a system that is similar to IPP. I comment about the tests he describes below.

8. Tests Conducted by Paige and Bunting

Having reviewed declaration Exhibit 5 and expert report Exhibit 6 of Patrick Page, and the declaration of Stephen Bunting, I can confirm the following.

The tests described by Paige and Bunting are trivial tests that set up three or four test computers with installed BitTorrent clients connected to Internet service providers configured to share a small number (e.g. 4) predetermined video files using BitTorrent. These simplistic "demonstration tests" confirm that all the pieces of the videos were detected and captured by IPP. However, the IPP system's operating workload at the time of the tests, and the workload conditions in the BitTorrent swarm were not described. And their tests did not document the operating workloads or churn among peers participating in the BitTorrent swarm during the period of the testing.

Paige and Bunting's tests demonstrate nothing about the reliability of the IPP software when operated under real-world operating conditions. They have not attempted to address the problems associated with routers using dynamic IP addressing (i.e. IP address resets), or conduct tests that attempt to determine if more than one user is attached to the router, or that the user has aborted an unintended download, or that a user has shut down because all the pieces of a movie have been received from other users in the swarm.

At the very least, these tests should have simulated router resets by powering them down and rebooting them during file sharing, and by running scenarios where BitTorrent users abort the downloading of shared video files before completion. Such operationally representative tests would have confirmed whether the IPP software could cope with unusual circumstances and events, and whether all the pieces of a video file could be received by users collaborating across an intensively active BitTorrent swarm.

9. Testing Conducted by Paige and Bunting as it Relates to Stalzer and Pasquale

9.1 Concerns Relating to Stalzer's Declaration and Deposition

Now relating Stalzer Exhibits 1 and 2 to testing conducted by Paige and Bunting, I can confirm:

a. None of the tests conducted by Paige or Bunting verified that "infringing files" (movies) were reliably transferred from the IPP system to the verification tool to support Stalzer's verification work;

b. Neither Paige nor Bunting conducted tests that the entirety of an "infringing file" associated with the IP address of a purported infringing user was transferred to the verification tool, that is, that an entire movie verified by Stalzer were indeed determined to have been captured from the purported infringer;

c. No tests were performed to verify that the *control copies* retrieved from the torrent website(s) used by Stalzer are actually owned by Strike 3, for example, by checking file hashes;

d. No tests were performed to verify that the "infringing file" and the control copy retrieved from the torrent website are computationally identical – this could be done by calculating and comparing file hashes;

Facts of the Matter: In the absence of successfully executed tests a., b., c. and d. above, the Plaintiff's experts (Paige and Bunting) have <u>not demonstrated</u> the following facts:

i. that infringing files were reliably transferred to the verification tool from IPP;

ii. that the entire file received by the verification tool was received from a single infringing user;

iii. that the control copy used by the verification tool was actually owned by Strike 3.

Given these facts, IPP may well have been routinely delivering false positive reports to Stalzer.

Additional Findings: Brandon Garcia-Paeth (Exhibit 8) and Kal Toth (Exhibit 9) confirm that in the present case, IPP downloaded at most 2 pieces (0.007%) of each of the purportedly infringed files from the Defendant's IP address. This raises several serious questions:

#1 By way of the verification tool, how could Stalzer have successfully played the "infringed file" delivered by IPP given that IPP reported detecting only a tiny fraction (0.007%) of the file?

#2 Could it be that IPP actually delivers an infringed file collected from many BitTorrent users?

#3 Could it be that IPP actually delivers a playable copy that is not acquired by way of BitTorrent?

These findings additionally undermine assertions by IPP's experts that IPP is a reliable forensics tool.

9.2 Concerns Relating to Pasquale's Declaration and Deposition

Now relating Pasquale Exhibits 3 and 4 to testing conducted by Paige and Bunting, I can confirm:

a. None of the tests conducted by Paige or Bunting verified that the PCAPs and declarations provided to Pasquale were reliably transferred to him from IPP by way of the Jira tool.

b. Neither Paige nor Bunting's tests verify how many PCAPs have been collected from a purported infringer and delivered to the PCAP verifier.

Facts of the Matter: In the absence of successfully executed tests a. and b. above, the Plaintiff's experts (Paige and Bunting) have not demonstrated the following facts:

i. that PCAP files and declarations are reliably transferred from IPP to Pasquale over Jira for PCAP verification, ISP lookup, signature, and submission back to Paul;

ii. that all the PCAPs necessary to assemble a complete/playable movie were received, verified (PCAP and ISP), signed, and submitted to IPP (via Jira and Paul).

Given these facts, Pasquale could be routinely receiving faulty PCAP files and declarations.

Additional Findings: Brandon Garcia-Paeth (Exhibit 8) and Kal Toth (Exhibit 9) confirm that in the case of the Defendant, IPP downloaded at most 2 pieces (0.007%) of each of the purported 80 to 87 files alleged to have been infringed. This raises the following concern about IPP's business model:

Stalzer's task attempts to verify that an infringed movie file can be viewed in its entirety, and compared to a control copy, prior to Stalzer signing a declaration that asserts infringement.

In stark contrast, Pasquale's task verifies PCAPs collected from purportedly infringing BitTorrent users. The verifier completes, signs, and submits a declaration in preparation for a possible request to issue a subpoena, and action that is launched immediately upon receiving the first PCAP of a movie from IPP.

These verification efforts of Stalzer and Pasquale appear to be at odds with each other.

My rate is $350.00 per hour.

K. C.

Signed under the Penalty of Perjury,

Kal Toth (Kalman C. Toth), Ph.D., P.Eng.

Exhibit 1

Declaration of Susan B. Stalzer in Support of Plaintiff's Motion for Leave to Serve a Third Party Subpoena Prior to Rule 26(f) Conference, Case No.: 2:17-cv-01731-MJP, Document 4-5, filed 11/29/17.

The Honorable Marsha J. Pechman

UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF WASHINGTON

AT SEATTLE

STRIKE 3 HOLDINGS, LLC, a Delaware corporation, Plaintiff, vs. JOHN DOE subscriber assigned IP address 73.225.38.130, Defendant.	Case No.: 2:17-cv-01731-MJP **DECLARATION OF SUSAN B. STALZER IN SUPPORT OF PLAINTIFF'S MOTION FOR LEAVE TO SERVE A THIRD PARTY SUBPOENA PRIOR TO A RULE 26(f) CONFERENCE**

[Remainder of page intentionally left blank]

EXHIBIT D

DECLARATION OF SUSAN B. STALZER IN SUPPORT OF PLAINTIFF'S MOTION FOR LEAVE TO SERVE A THIRD PARTY SUBPOENA PRIOR TO A RULE 26(f) CONFERENCE

I, Susan B. Stalzer, do hereby state and declare as follows:

1. My name is Susan B. Stalzer. I am over the age of 18 and am otherwise competent to make this declaration.

2. This declaration is based on my personal knowledge and, if called upon to do so, I will testify that the facts stated herein are true and accurate.

3. I work for Strike 3 Holdings, LLC ("Strike 3") and review the content of their motion pictures.

4. I hold a Bachelor's degree and Master's degree in English from Oakland University.

5. I have a long history of working in the fine arts, with an emphasis on writing, including having served as an adjunct professor of composition and literature.

6. I am familiar with Strike 3's plight with online piracy and its determination to protect its copyrights.

7. I was tasked by Strike 3 with verifying that each infringing file identified as a motion picture owned by Strike 3 on torrent websites was in fact, either identical, strikingly similar or substantially similar to a motion picture in which Strike 3 owns a copyright.

8. IPP provided me with the infringing motion picture file for each of the file hashes listed on Exhibit A to Strike 3's Complaint.

9. I viewed each of the unauthorized motion pictures corresponding to the file hashes side by side with Strike 3's motion pictures, as published on the *Blacked*, *Tushy* and/or *Vixen* websites and enumerated on Exhibit A by their United States Copyright Office identification numbers.

10. Each digital media file, as identified by the file hash value, is a copy of Strike 3's corresponding motion picture and is identical, strikingly similar or substantially similar to the

EXHIBIT D

original work identified by their United States Copyright Office identification numbers on Exhibit A to the Complaint.

DECLARATION

PURSUANT TO 28 U.S.C. § 1746, I hereby declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 20th day of November, 2017.

SUSAN B. STALZER

By: ____________________

EXHIBIT D

Exhibit 2

Extracted pages from the rough transcript of the deposition of Susan B. Stalzer deposition, 4/16/19, pp. 29, 33, 49, 58, 75, 76,118, 133, 138, 140, 141

THIS IS AN UNCERTIFIED ROUGH DRAFT
AND CANNOT BE QUOTED IN ANY PLEADINGS
OR USED FOR ANY PURPOSE OTHER THAN
CASE PREPARATION AND MAY NOT BE
FILED WITH ANY COURT

This uncertified rough draft has not been proofread and may contain untranslated stenographic symbols, an occasional reporter's note, a misspelled proper name and/or nonsensical word combinations. All such entries will be corrected on the final certified transcript.

Due to the need to correct entries prior to certification, you agree to use this draft only for the purpose of augmenting counsel's notes and not to use or cite it in any court proceeding.

Please keep in mind that the final certified transcript page and line numbers will not match the rough draft due to the not clear to me.

Q. Okay. Well, let's walk through it.

First day you got this job at -- for Strike 3 Holdings, how did you verify the first work?

A. We have a verification tool in which I can play the clips.

Q. Okay. What is the name of that verification tool?

A. Verification tool.

Q. Okay. Who made the verification tool?

A. I have no idea.

Q. How do you know the verification tool works?

MR. BANDLOW: Objection. Vague and ambiguous.

THE WITNESS: It works in what regard? I don't understand the question.

and you open up the verification system.

A. Correct.

Q. What's the first thing you see when you open up the verification system?

A. A list of hash marks. A list of the site that the film is purported to be coming from, the title that is believed to be attached to this film and a button where I can hit play for the film to pop up for me to view it.

Q. Okay. And how is that information organized?

MR. BANDLOW: Objection. Vague and ambiguous.

THE WITNESS: Often alphabetically by title.

BY MR. EDMONDSON:

Q. Okay. Is it organized by case?

A. No, sir.

(Whereupon, the record was read.)

THE WITNESS: It's my understanding that the productions that they put out, they own copyrights on.

BY MR. EDMONDSON:

Q. How is that your understanding?

A. Because they are branded as their material. I guess I'm not sure how to answer that more clearly.

Q. Okay. So you have seen a number of the Strike 3 Holdings movies?

A. I have.

Q. Okay. And where on the movies does it say Strike 3 Holdings?

A. Okay. Fair enough. I know they're owned by the sites. The connection between the websites where the movies are put forth for membership in viewing versus Strike 3's relationship with that copyright, I have no knowledge.

Q. Okay. So you talked about the websites. Did you ever see the words have enter a user ID and password?

A. Yes.

Q. And what is that user ID and password?

MR. BANDLOW: That's confidential.

MR. EDMONDSON: We can mark it as confidential.

THE WITNESS: It's independent to me.

BY MR. EDMONDSON:

Q. I'm not asking what it's independent to. I'm asking what your user ID and password is.

MR. BANDLOW: We're not going to give that. I'll instruct the witness not to answer. It's her user ID and password. So we're not going to give that to you.

MR. EDMONDSON: There's nothing privileged about the user ID and password.

MR. BANDLOW: I'm still not going to give that to you based on your history with harassing her, so, no, you're not getting it. So next question.

MR. EDMONDSON: It's not her property, it's the property of Strike 3 Holdings.

MR. BANDLOW: I understand, but I'm

marked Page 3. Have you ever described yourself as a comparer?

A. I think it's a fair description.

Q. Okay. But did you talk to anybody -- well, have you ever seen this text here before?

A. I did not.

Q. You did not draft this information here?

A. No, sir.

Q. So you didn't tell someone at Fox Rothschild that you're a comparer?

A. No.

MR. BANDLOW: We came up with that lovely word, Curt. We're very proud of it.

BY MR. EDMONDSON:

Q. And you see here, possesses information that the motion pictures identified by their cryptographic hash value on the BitTorrent network that defendant's IP address infringed correspond to motion pictures owned by Strike 3.

Now, we just looked at Document 62 there, correct --

A. Correct.

Q. -- the screen of the verification system?

Is there an IP address anywhere on that screen?

A. Not that I have, no.

Q. And do you know of any IP addresses in this case?

A. No.

Q. Do you know of any IP addresses in any case?

A. No.

Q. Do you know your own IP address?

A. Not offhand, no.

Q. Let me hand you a document marked Exhibit 45. Miss Stalzer, have you seen this document before?

A. No.

Q. Have you ever seen a complaint in any

Conference?

A. Yes, I see that.

Q. So when -- did you, when you signed this declaration, did you read that caption?

A. I'm not given the cover pages when the declarations are sent to me.

Q. I see. So you don't know if it's for a particular case, correct?

A. I don't have the case number that's attached.

Q. Okay. How many declarations have you signed?

A. I don't know exactly.

Q. Well --

A. From your own information, it seems to be over 3,000.

Q. Does that seem right?

A. Yes, sir.

Q. From Oakland University?

A. Yes.

Q. Would you say your command of the English language is probably better than the average person's?

MR. BANDLOW: Objection. Calls for speculation. Vague and ambiguous.

Go ahead and answer.

THE WITNESS: I don't know that I'm arrogant enough to put myself above and beyond other people. I feel I have a reasonable command of the English language.

BY MR. EDMONDSON:

Q. Okay. Now, the sentence IPP provided me with the infringing motion picture file, did IPP provide you with the infringing motion picture file?

A. Through the verification tool, yes.

Q. But that's not what that says. It doesn't say IPP provided me with the infringing motion picture file through the verification

A. Again, it would vary depending on the situation. There have been times more often than direct communication between Tobias and myself, Sud will communicate with me and copy Tobias or communicate with Tobias and copy me, "When is the next batch being uploaded," something to that effect.

Q. And what's Tobias's e-mail address?

A. I don't know off the top of my head.

Q. But IPP did not provide you with the infringing motion picture, the verification system provides you with that?

A. They have to get there somehow. They have to get into the verification tool some way, and IPP is the way in which they are loaded into the verification tool.

Q. But there's nothing on the verification tool that says IPP on it, correct?

A. Not to my knowledge.

Q. Okay. Now, looking at Paragraph 9 of this declaration, do you see reference to Exhibit A?

A. Yes.

for me.

BY MR. EDMONDSON:

Q. Now, going back to Exhibit 62 [Sic], and you see Paragraph 10 on your declaration, how do you note whether the motion picture and the digital media file is identically identical or strikingly similar or substantially similar?

A. Through the number of different ways I use to verify, as I had stated earlier.

Q. Yeah, but those are three different categories. So do you have a notation system of determining which of these works were identical, which were strikingly similar and which were substantially similar?

A. No.

Q. How do you distinguish between those three characteristics?

A. I do not have a measure with which to grade between those three categories. I guess the only way I know how to answer that question is that before I will verify something is good, that I am confident that they are the same film.

Q. Okay. But you used three words in this declaration.

A. The declaration states three different ways.

Q. The declaration states three different characteristics, or three different analysis, identical, strikingly similar or substantially similar.

What I'm asking is how do you characterize each of those three species?

MR. BANDLOW: Objection. Asked and answered.

Try again.

THE WITNESS: I don't particularly

Exhibit 3

Declaration of John S. Pasquale in Support of Plaintiff's Motion for Leave to Serve a Third Party Subpoena Prior to Rule 26(f) Conference, Case No.2:17-cv-01731-MJP, Document 4-4, filed 11/29/17

The Honorable Marsha J. Pechman

UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF WASHINGTON

AT SEATTLE

STRIKE 3 HOLDINGS, LLC, a Delaware corporation, Plaintiff, vs. JOHN DOE subscriber assigned IP address 73.225.38.130, Defendant.	Case No.: 2:17-cv-01731-MJP **DECLARATION OF JOHN S. PASQUALE IN SUPPORT OF PLAINTIFF'S MOTION FOR LEAVE TO SERVE A THIRD PARTY SUBPOENA PRIOR TO A RULE 26(f) CONFERENCE**

[Remainder of page intentionally left blank]

EXHIBIT C

DECLARATION OF JOHN S. PASQUALE IN SUPPORT OF PLAINTIFF'S MOTION FOR LEAVE TO SERVE A THIRD PARTY SUBPOENA PRIOR TO A RULE 26(f) CONFERENCE

I, John S. Pasquale, do hereby state and declare as follows:

1. My name is John S. Pasquale. I am over the age of 18 and I am otherwise competent to make this declaration.

2. This declaration is based on my personal knowledge and, if called upon to do so, I will testify that the facts stated herein are true and accurate.

3. I am a Senior Project Manager with 7 River Systems, LLC a Maryland based cyber security firm specializing in network security, data breaches, and the protection of secured information transmitted across networks.

4. For over 30 years, I have worked in the IT industry, specializing in system and network administration and project management.

5. I have consulted and advised major financial institutions and Fortune 500 companies on the management, security and implementation of major data centers, delivering complex and large scale network projects.

6. I was retained by Strike 3 Holdings, LLC ("Strike 3") to individually analyze and retain forensic evidence captured by IPP International U.G. ("IPP").

7. I received a PCAP from IPP containing information relating to the transaction occurring on 09/05/2017 10:40:33 involving IP address 73.225.38.130.

8. I used a program called Wireshark to view the contents of the PCAP.

9. I was able to confirm that IPP recorded the transaction with 73.225.38.130 at 09/05/2017 10:40:33.

10. Based on my experience in similar cases, Defendant's ISP Comcast Cable is the only entity that can correlate the IP address to its subscriber and identify Defendant as the person assigned the IP address 73.225.38.130 during the time of the alleged infringement. Indeed, a subpoena to an ISP is consistently used by civil plaintiffs and law enforcement to identify a subscriber of an IP address.

DECLARATION

PURSUANT TO 28 U.S.C. § 1746, I hereby declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 24th day of November, 2017.

JOHN S. PASQUALE

By:

Exhibit 4

Extracted pages from the rough transcript of the deposition on John S. Pasquale, 04/17/19, pp. 25-28, 33-36, 37-38, 42-45, 53-54, 72-74

(INSERT CAPTION/APPEARANCES/INDEX/SWORN)

STARTTIME9:40AM 4/17/19

(EXHIBIT MARKED/70)

Q Good morning, Mr. Pasquale.

A Good morning.

Q Could you please state and spell your name for the record?

A John Pasquale, J-o-h-n, P-a-s-q-u-a-l-e.

Q Do you have a middle name?

A Yes, Santo, S-a-n-t-o.

Q Excellent. Mr. Pasquale, have you ever been deposed before?

A No, I have not.

Q Some of the grounds rules for a deposition is the Court Reporter is taking down our words, so if you can answer verbally, that would be appreciated. She can't record gestures.

A Understood.

Q If you nod yes or shake no, she can't take that down.

A Understood.

Q Do everything verbally. The other thing, too, is that I might ask you to either to estimate some things, so what I'd like to you do

Q Do you know the IP address for your router?

A No.

Q Do you ever analyze any of these PCAPs on a laptop?

A No.

Q So you keep everything on your computer?

A Yes.

Q While you're doing this PCAP analysis, are you making any notes of your analysis?

A No.

Q When you're done analyzing the PCAP, what do you do with it?

A I upload it to a program called JIRA, which is a workflow application and send them off to Paul for review.

Q JIRA?

A J-I-R-A.

Q The PCAP comes in from -- is it Paul?

A Yes.

Q Is that attached to an email?

A No, it's through JIRA.

Q So you have a JIRA application. Who is on the JIRA application?

A I'm not sure I understand the question.

Q Explain JIRA to me.

A So JIRA is a workflow application. In this case PCAPs and declarations are attached to a particular case. Then from there I pull up those two documents and analyze, sign and save.

Q You get the declaration and the PCAP. Are they both together in the same --

A They're together in the same case, yes.

Q Just so the record is clear, when we use the word "case," in the legal profession we're usually referring to something like a lawsuit. When you're using the word "case," what do you mean?

A When I'm using the word "case," it is one declaration and one PCAP.

Q In the JIRA?

A Yes.

Q Is there any notation that says this is for a lawsuit number, and in this case 2:17-cv-01731?

A There are numbers attached to it. I'm not sure if they coincide with a lawsuit.

Q When is the last time you looked at the JIRA app?

A Three days ago.

Q Describe what you saw in that last transaction?

A So the case, what I'm calling the case would have a number associated with it, an abbreviation of a district, what state that it's in, and then the actual district within the state, and I believe that's it.

Q Is the number a four-digit number?

A Yes. I believe so, yes.

Q Then when you get it in on JIRA, do you save the PCAP to your desktop?

A Yes.

Q Do you save the declaration to the desktop?

A Yes, on a temporary basis. I don't save the PCAP. I save the declaration.

Q You put the declaration on your desktop?

A I save it locally, and then I upload it, and then once I'm done, I delete it from my desktop.

Q Were you ever given instructions by Paul not to delete data?

A No.

Q Were you ever given instructions by Paul to organize the data that you analyze on your system in some directories or folders by the four-digit case number?

A In my system, no.

Q So Paul never said to you to keep a record of the analysis that you have done in these cases. Is that correct?

A No. The records are stored on JIRA. That's what JIRA is for.

Q I understand, but my question was, did he ask you to keep a local independent record of the analysis that you did?

A No.

Q So as we speak right now, the only record that you have of your analysis would be the transactions and JIRA?

A Correct.

Q And obviously the declarations filed in the courts. Correct?

A Say that again.

Holdings, LLC produced on the internet, via the internet?

A Before I signed any declaration, it was explained to me by Paul exactly what Strike 3 is. In fact, he consulted with me on whether or not to take on the client, and that was our conversation about Strike 3 and what they do.

Q Did Paul tell you not to do any independent research into Strike 3 Holdings?

A No.

Q So you didn't have the natural curiosity to go out and google "Strike 3 Holdings"?

A I'm a very busy man.

Q But you've signed hundreds of declarations for Strike 3 Holdings. True?

A Yes.

Q Let's go to the next line. Do you see line 26 there? Do you see that phrase, "Indeed, a subpoena to an ISP is consistently used by civil plaintiffs and law enforcement to identify a subscriber of an IP address."

What is your experience with subpoenas?

A None.

Q Why did you use that word in there?

A Well, to me a subpoena is a document through the courts to go to an ISP and obtain an IP address and who that IP address belongs to.

Q The statement is, "Indeed, a subpoena to an I SP is consistently used by civil plaintiffs and law enforcement to identify a subscriber of an IP address."

What experience do you have that supports that statement that you made there?

A I know that you would need some type of court order to obtain an IP address.

Q How do you know that?

A Through my experience in the IT industry.

Q What experience has that been?

A It's 35 years of experience.

Q Have you ever worked for an attorney on a subpoena to an ISP?

A No, I have not.

Q Have you ever actually drafted a subpoena going to an ISP?

A No, I have not.

Q What engagements did you ever deal with subpoenas going to ISP's?

A None.

Q So I want to -- when you say the word there "indeed, a subpoena," that suggests to me a very clear affirmative statement that you've done this a lot, but my understanding is you've never participated in sending subpoenas to an ISP. Is that correct?

A I have not. You're probably misinterpreting that line.

Q I want to know why you wrote it.

A I wrote it because it's my understanding that a subpoena is needed to go to a -- a court order is needed in order to get an actual person attached to an IP address, through the ISP.

Q Did you draft this sentence? Did you sit down at a computer --

A No, I did not.

Q Who drafted this sentence?

A This was given to me by 7 Rivers.

Q Do you know if Paul drafted this sentence?

A I don't know.

Q I want you to turn to the next page please. Do you see the declaration there at the top?

A Yes.

Q And do you see there, "Pursuant to 28 U.S.C. 1746"?

A Uh-huh.

Q What's your understanding of the next sentence, "I hereby declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct"?

A That anything that I'm saying here -- that anything that is said in this document that I'm signing, that it's true and correct.

Q How do you know this is true and correct?

A I know it's true and correct by the PCAP that I reference.

Q I mean, going back to Line 26 and 27. From experience?

A From experience.

Q But you didn't draft that statement?

A No, I did not.

Q And you testified earlier that you've never had experience sending subpoenas to ISPs?

A That's correct.

Q You testified earlier -- and I want to make sure. In Paragraph 7 of your declaration you said, "I received a PCAP from IPP," but I understood you received a PCAP from Paul on JIRA.

A Correct.

Q So why doesn't that sentence say, "I received a PCAP from Paul on JIRA containing information relating to the transaction"?

A I would assume that 7 Rivers Systems is the handler, but the original document comes from IPP.

Q That's an assumption. Correct?

A Yeah, I guess so.

Q So Paragraph 7 did you -- you didn't draft Paragraph 7?

A As I said, I didn't draft this document. I reviewed the document. I look at the content of the document. I ensure that the content in the document is correct according to the PCAP, and then from there sign it.

Q What I'm trying to do is find out if there's any inaccuracies in this document so, in Paragraph 7 you didn't receive a PCAP from IPP. You received the PCAP from Paul using the JIRA system. Correct?

A Sure, you can say that, but the document originates from IPP and Strike 3 Holdings.

Q How do you know that?

A Because Strike 3 Holdings is the client of 7 Rivers Systems.

Q Do you do computer forensics?

A Actually, that's what this is.

Q And so you're familiar with concepts of chain of custody?

A Sure.

Q Did you verify the chain of custody of this data coming from IPP to 7 Rivers Systems to your JIRA and then to your desktop? Did you verify every step?

A No, I did not.

(EXHIBIT MARKED/73)

Q I'm going to hand you a blank sheet marked 73. Can you sketch out the system architecture of the IPP monitoring system to the best of your knowledge?

A I cannot.

Q Can you describe then for me in your best understanding what the IPP system does?

A No.

Q Do you know where it's located?

A I believe they're in Germany, but I'm not a hundred percent sure.

Q Did you ever ask to visit the IPP facility?

A No.

Q Did you ever ask to speak to anybody at IPP?

A No.

Q Why not?

A It's not part of my job description. It's above my pay grade.

Q Do you know that these declarations have been used in lawsuits?

A Yes.

Q Have you ever been sued?

A No.

Q What data inside the PCAP would suggest to you that it came from IPP?

A What data?

Q Right.

A None.

Q There's nothing in the PCAP that it came from IPP?

A I don't believe so.

Q In your analysis -- going to Paragraph 10, do see Line 23 there on the declaration we've marked as Exhibit 71?

A Uh-huh.

Q "Based on high experience in similar cases."

What other similar cases were you referring to when you said that?

A Other cases that have PCAPs and use Comcast as the ISP.

Q Well, defendant's ISP, Comcast Cable, how did you know it was Comcast?

A There's a program that you can run the IP address, and it will tell you exactly who the ISP is.

Q Did you run that program?

A Yes, I did. For this one I believe I did, yes.

Q What's the program?

A I don't have it off the top of my head, but I can certainly send it to you if you like. You can look it up and google it, and probably 4,000 will come up.

Q When you did this analysis you

looked at JIRA. Right? You got the PCAP and the declaration from JIRA?

A Correct.

Q And you also took and copied -- and correct me if I'm wrong. You copied the IP address into this other program to look up who the cable provider is. Correct?

A Who the ISP is.

Q And then what did you do? A screen print of that?

A No.

Q How did you confirm that that was Comcast?

A I confirmed what was in the documents stating that the defendant's ISP was Comcast because it was already written there. As I said, I did not draft these documents. I'm verifying the documents.

Q You verified it using a program, but you didn't keep a record of your verification?

A No, I did not.

Q Did you have like a?

A This is the record of my verification.

Q Did you have a notebook or

spreadsheet that would say --

A No.

Q What happened if you got -- if it didn't verify? What would you do?

A I would reject the declaration.

Q How many of these declarations have you rejected?

A At first there was quite a few. I can't give you an exact amount, but at first I would say ten percent, maybe more. I don't know. I don't recall.

Q Did you make notes in JIRA --

A Yes.

Q -- on those rejections?

A Yes, I did.

Q So when you saw rejections, did you ask Paul -- is that your son?

A Uh-huh.

Q Did you ask Paul, Why are we getting these rejections?

A Only if it was at a high rate, and there was one point where there was a high rate, but it wasn't due to the wrong ISP. It was more toward the time stamp itself.

(EXHIBIT MARKED/45)

A I would surmise that it would be Paul if he did.

Q It's a small company.

A Yes.

Q It's a family-run company.

A I don't know if it's family run, but it's run by my son.

Q Before I became a lawyer, I was in the software business with my dad, so I'm familiar with the setup.

Now that you know that 80 works were alleged to have been infringed --

A I know that because you just told me, but go ahead.

Q This is a Complaint filed by your customer, strike 3 Holdings, something your customer drafted, not me. Now that you know that 80 works were alleged to have been infringed and now that you've established your professional and cyber investigations --

A You can label it that.

Q If I labeled it incorrectly, please let me know.

A That's fine.

Q Would you have requested PCAPs on

these other 79 works?

A If I would have known that they were all interconnected? I don't know to be honest. I would just be -- I would ask for counsel's guidance.

Q Would you consider your investigation to be thorough if you only looked at one out of 80 PCAPs?

A Yes.

Q Let's explore that. Do you see under the UTC column where it says 9/5/2017?

A Yes.

Q And you testified earlier and you filed a declaration saying you know something about Comcast Cable. Correct?

A Uh-huh.

Q And do you know if this IP address supplied by Comcast Cable was static or dynamic?

A Don't know.

Q Do you understand the difference between a static and dynamic IP address?

A Yes.

Q Explain to me the different between a static and a dynamic IP address.

A A static IP address is one that's

A No, I did not.

Q You didn't look up the source IP address?

A No.

Q Is there anything about that source IP address that is unusual?

MR. ATKIN: Objection to form. You can answer if you understand.

A No.

Q You're familiar with the internet topology?

A Yes.

Q Are you familiar with nonroutable IP addresses?

A Nonroutable IP addresses? To a certain extent.

Q I probably slurred my words. Nonroutable IP address?

A Okay.

Q When you studied internet topology, were you aware of blocks of IP addresses that are designated as not allocated to a particular computer?

A I'm not sure I understand your question.

Q You understand in the network architecture of the internet that every computer is assigned an IP address?

A Correct.

Q And since there's billions of computers, there's not enough IP addresses to go around. Correct?

A Yes.

Q And so the way the internet has been organized is that behind routers they will have internal IP?

A Nonregistered IP addresses.

Q And then for everybody to communicate across the internet, you have actual IP addresses?

A Correct.

Q And there's blocks of IP addresses that have been designated that won't route to the outside internet?

A Correct.

Q Otherwise everything would be blow up?

A It would be mayhem, yes.

Q Do you know what those blocks of nonroutable IP addresses are?

A No.

Q If that IP address turns out to be nonroutable, would it have changed your analysis and your declaration?

MR. ATKIN: Objection. What is that IP address?

Q Let's put it on the record now that you brought that up. Can you read off the IP address of Line 2 there?

MR. EDMONDSON: If you can confirm it counsel because I'm not looking it?

A 192.168.0.13.

MR. ATKIN: He asked for Line 2.

THE WITNESS: This is Line 2, destination.

Q In this transactions, there's two IP addresses. Correct?

A Uh-huh.

Q Because we have this computer communicating with --

A Yes.

Q So in this transaction we don't see three or four IP addresses. It's just --

A Per transaction within the PCAP.

MR. EDMONDSON: Off the record

Exhibit 5

Declaration of Patrick Paige, S3H (217-cv-01731)_000166, filed 11/12/13

DECLARATION OF PATRICK PAIGE

I, PATRICK PAIGE, DO HEREBY DECLARE:

1. I am over the age of eighteen (18) and otherwise competent to make this declaration. The facts stated in this declaration are based upon my personal knowledge.

2. I was a police officer from 1989 until 2011 for the Palm Beach County Sherriff's Department. And, from 2000-2011, I was a detective in the computer crimes unit.

3. As a detective in the computer crimes unit, I investigated internet child pornography and computer crime cases.

4. I have conducted forensic computer examinations for:

(a) Broward County Sheriff's Office (BSO);

(b) Federal Bureau of Investigation (FBI);

(c) U.S. Customs and Border Protection (CBP);

(d) Florida Department of Law Enforcement (FDLE);

(e) U.S. Secret Service;

(f) Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); and

(g) Various municipalities in the jurisdiction of Palm Beach County.

5. I was also previously assigned to a police unit working in conjunction with TLO Corp., which is a private company.

6. When I worked with TLO Corp., I supervised the other detectives assigned to the unit, which was consisted of six online investigators and two computer forensic examiners.

7. I am familiar with software programs used to investigate computers, including EnCase and Access Data.

8. I have taken over 400 hours of courses designed to teach people how to investigate computers.

9. Also, while working from 2003-2011 for Guidance Software, the makers of EnCase, I have taught over 375 hours of courses in computer forensics ranging from beginner to advanced levels.

10. I have had students in my courses from various government branches, including: (a) sheriff's offices; (b) FBI agents; (c) ATF agents; (d) agents from the Central Intelligence Agency, and (e) individuals from other branches of government and the private sector.

11. After leaving the Palm Beach County Sherriff's office, I founded Computer Forensics, LLC, where I am currently employed.

12. I have received the following awards and commendations:

(a) 1991 – Deputy of the Year, awarded by the 100 Men's Club of Boca Raton & Rotary Club.

(b) 1997 – Deputy of the Month for June.

(c) 2001 – Detective of the Month for October.

(d) 2002 – Outstanding Law Enforcement Officer of the Year, awarded by the United States Justice Department for work in the *U.S. vs. Jerrold Levy* case.

(e) 2003 – U.S. Customs Service Unit Commendation Citation Award for computer forensic work in Operation Hamlet. Operation Hamlet was one of the largest rings in the history of U.S. Customs of individuals who were molesting their own children, and transmitting the images and video via the Internet.

(f) 2005 – Detective of the Month for December.

(g) 2007 – Outstanding Law Enforcement Officer of the Year, awarded by the United States Justice Department for work in the *U.S. vs. Jimmy Oliver* case.

(h) 2008 – Letter of Commendation issued by the FBI for outstanding computer forensic work in the *U.S. vs. Frank Grasso* case.

13. I have been called to testify as a fact and expert witness on numerous occasions in the field of computer forensics in both trial-level and appellate proceedings before state, federal, and military courts in Florida, California, New Jersey, and New York.

14. No court has ever refused to accept my testimony on the basis that I was not an expert in computer forensics. My skill set and my reputation are my most important assets in my current position with Computer Forensics, LLC.

15. With regard to my experience investigating child pornography cases, I supervised police officers whose responsibility it was to establish a successful TCP/IP connection with persons who were sending pornographic images of children or other illegal content over the Internet.

16. The offenders' IP addresses, as well as the dates and times of the illegal transmission were recorded.

17. An officer would then request that the assistant state attorney subpoena the corresponding ISPs for the purpose of identifying the subscribers that were transmitting the illegal content.

18. In these cases, the subscribers were not notified by the ISPs that their identity was being subpoenaed because they could have deleted the images and destroyed the data.

19. After receiving the subscribers' identities, we would prepare a search warrant that would authorize us to enter the subscribers' dwelling and seize all of their computer devices.

20. I was directly involved in approximately 200 search warrants either by way of managing the process or performing it personally.

21. I can recall only one instance in all the times that we executed a search warrant and seized computers where we did not find the illegal content at the dwelling identified in the search warrant.

22. In that one instance, the Wi-Fi connection was not password protected, and the offender was a neighbor behind the residence.

23. I never came across a Wi-Fi hacker situation.

24. In my opinion, a child pornographer has a greater incentive to hack someone's Wi-Fi connection than a BitTorrent user because transmission of child pornography is a very serious crime with heavy criminal penalties, and many offenders can face life sentences if convicted.

25. I tested IPP International U.G.'s ("IPP") IP detection process.

26. To do so, I downloaded four public domain movies from the national archive.

27. I then encoded text into the videos, so that I would know whether someone that downloaded that particular movie downloaded the version of the movie that I created.

28. I then rented four virtual servers, each of which was connected to the Internet and used a unique IP addresses.

29. I then configured the servers so that all of them were running Windows 2008 server edition, and I put a different BitTorrent client onto each server.

30. A BitTorrent "client" is software that enables the BitTorrent protocol to work.

31. After installing the BitTorrent clients, I also installed Wireshark onto each server. "Wireshark" is a program that captures network traffic and creates PCAPs, just as TCP Dump, which IPP uses, does. A PCAP is like a video recording of all the incoming and outgoing transactions of a computer.

32. After installing Wireshark onto each of the servers, I transferred the movies from my local computer to the servers.

33. I then used the BitTorrent clients on each of the servers to make .torrent files. I uploaded these .torrent files onto various torrent websites.

34. I then informed IPP of the movie names. Thereafter, IPP sent me screen captures of the movies I had seeded.

35. The screen captures sent by IPP had my codes on them; thus, I knew that IPP had caught the movies I had seeded.

36. IPP also sent me additional data identifying the IP Address used by each of the four servers, and sent me PCAPs.

37. I reviewed IPP's PCAPs vis-à-vis the PCAP log files created by each of my test servers, and determined that IPP's PCAPs match my PCAPs. This could not have happened unless IPP's server was connected to the test server because the transactions would not match.

38. From this test, I concluded that IPP's software worked, and had a subpoena been issued for my IP addresses, it would have revealed my identity.

FURTHER DECLARANT SAYETH NAUGHT.

DECLARATION

PURSUANT TO 28 U.S.C. § 1746, I hereby declare under penalty of perjury that the foregoing is true and correct.

Executed on this 11th day of November, 2013.

By: Patrick Paige
Digitally signed by Patrick Paige
DN: cn=Patrick Paige, o=Computer Forensics LLC, ou, email=patrick@patrickpaige.com, c=US
Date: 2013.11.11 15:53:41 -05'00'

PATRICK PAIGE

Exhibit 6

Expert Report Regarding Testing of IPP International UG's Infringement Detection System (Exhibit B), Patrick Paige Computer Forensics LLC, S3H (217-cv-01731)_000171, filed 11/06/18

Computer Forensics, LLC
1880 N. Congress Ave Suite 333
Boynton Beach, FL 33426
Main: 561.404.3074
www.ComputerForensicsLLC.com

EXPERT REPORT REGARDING TESTING OF IPP INTERNATIONAL UG'S INFRINGEMENT DETECTION SYSTEM

Prepared By: Patrick Paige, EnCE SCERS
Managing Member
Computer Forensics, LLC

Exhibit B

DECLARATION OF PATRICK PAIGE

I, PATRICK PAIGE, DO HEREBY DECLARE:

1. I am over the age of eighteen (18) and otherwise competent to make this declaration. The facts stated in this declaration are based upon my personal knowledge.

2. I was a police officer from 1989 until 2011 for the Palm Beach County Sherriff's Office. And, from 2000-2011, I was a detective in the Computer Crimes Unit. After leaving the Palm Beach County Sherriff's Office, I founded Computer Forensics, LLC, where I am currently employed.

3. I have taken over 400 hours of courses designed to teach people how to conduct computer forensic examinations.

4. Also, while working from 2003-2011 for Guidance Software, the makers of EnCase, I taught over 375 hours of courses in computer forensics ranging from beginner to advanced levels.

5. As a computer crimes detective for the Palm Beach County Sheriff's Office, I have conducted forensic computer examinations for:

(a) Broward County Sheriff's Office (BSO);

(b) Federal Bureau of Investigation (FBI);

(c) U.S. Customs and Border Protection (CBP);

(d) Florida Department of Law Enforcement (FDLE);

(e) U.S. Secret Service;

(f) Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); and

(g) Various municipalities in the jurisdiction of Palm Beach County.

6. I have had students in my courses from various government branches, including: (a) sheriff's offices; (b) FBI agents; (c) ATF agents; (d) agents from the Central Intelligence Agency; and (e) individuals from other branches of government and the private sector.

7. I have received the following awards and commendations:

(a) 1991 – Deputy of the Year, awarded by the 100 Men's Club of Boca Raton & Rotary Club.

(b) 1997 – Deputy of the Month for June.

(c) 2001 – Detective of the Month for October.

(d) 2002 – Outstanding Law Enforcement Officer of the Year, awarded by the United States Justice Department for work in the *U.S. vs. Jerrold Levy* case.

(e) 2003 – U.S. Customs Service Unit Commendation Citation Award for computer forensic work in Operation Hamlet. Operation Hamlet was one of the largest rings in the history of U.S. Customs of individuals who were molesting their own children, and transmitting the images and video via the Internet.

(f) 2005 – Detective of the Month for December.

(g) 2006 – Letter of Commendation issued by the FBI for outstanding computer forensic work in the *U.S. vs. Frank Grasso* case.

(h) 2007 – Outstanding Law Enforcement Officer of the Year, awarded by the United States Justice Department for work in the *U.S. vs. Jimmy Oliver* case.

8. I have testified as a fact and expert witness on numerous occasions in the field of computer forensics in both trial-level and appellate proceedings before state, federal, and military courts in California, Florida, Indiana, New Jersey, New York, and Pennsylvania.

9. No court has ever refused to accept my testimony on the basis that I was not an expert in computer forensics. My skill set and my reputation are my most important assets in my current position with Computer Forensics, LLC.

10. As part of my duties within the Computer Crimes Unit at the Palm Beach County Sherriff's Office, I investigated cases involving the use of the Internet, including cases involving peer-to-peer file sharing networks. In this role, I also investigated Internet child pornography and computer crime cases.

11. I was assigned to the Computer Crimes Unit that worked in conjunction with a private company called TLO Corp.

12. When I worked with TLO Corp., I supervised the other detectives assigned to the unit, which consisted of six online investigators and two computer forensic examiners.

13. In my experience, during the initial phase of Internet based investigations, the offender is only known to law enforcement by an IP address.

14. The only entity able to correlate an IP address to a specific individual at a given date and time is the Internet Service Provider ("ISP").

15. Once provided with the IP Address, plus the date and time of the detected and documented activity, ISP's can use their subscriber logs to identify the name, address, email address and phone number of the applicable subscriber in control of that IP address at the stipulated date and time.

16. With regard to my experience investigating child pornography cases, I supervised police officers whose responsibility it was to establish a successful TCP/IP connection with persons who were sending pornographic images of children or other illegal content over the Internet using peer-to-peer file sharing programs.

17. The offenders' IP addresses, as well as the dates and times of the illegal transmission were recorded.

18. An officer would then request that the assistant state attorney subpoena the corresponding ISPs for the purpose of identifying the subscribers that were transmitting the illegal content.

19. In these cases, the subscribers were not notified by the ISPs that their identity was being subpoenaed because they could have deleted the images and destroyed the data.

20. After receiving the subscribers' identities, we would prepare a search warrant that would authorize us to enter the subscribers' dwelling and seize all of their computer devices.

21. I was directly involved in approximately 200 search warrants either by way of managing the process or performing it personally while at the Computer Crimes Unit.

22. From my experience, Plaintiff is likely to identify the infringer. Indeed, during my time in the Computer Crimes Unit, I can recall only one instance in all the times that we executed a search warrant and seized computers, where we did not find the alleged illegal activity at the dwelling identified in the search warrant.

23. In that one instance, the Wi-Fi connection was not password protected, and the offender was a neighbor behind the residence.

24. I never came across a Wi-Fi hacker situation.

25. In my opinion, a child pornographer has a greater incentive to hack someone's Wi-Fi connection than a BitTorrent user because transmission of child pornography is a very serious crime with heavy criminal penalties, and many offenders can face life sentences if convicted.

26. The process used by law enforcement mirrors the process used by Malibu Media and IPP to correlate an IP address to an individual.

27. In order to ascertain the identity of the infringer, just as with law enforcement, Malibu Media must subpoena the ISP to learn the subscriber's true identity.

28. I tested IPP International U.G.'s ("IPP") infringement detection system. The infringement detection system is named "Observer." It is owned and used by IPP to identify individuals who are illegally downloading and distributing content via BitTorrent. This technology and similar investigative methods are used by law enforcement officials when tracking individuals who transmit contraband files such as child pornography via the Internet.

29. I tested IPP's infringement detection system for its accuracy in detecting and recording infringement via BitTorrent, ascertaining an infringing IP address[1], and identifying the "test" files being distributed on BitTorrent.

30. To conduct this test, I first downloaded four public domain movies from the national archive.

31. I then encoded text into each video. The purpose of this encoding was to ensure that when the file is located and download by IPP, it could be easily identified as the videos I personally encoded and seeded.

32. I then setup and configured four computers, each of which was connected to the Internet and each computer was configured with its own unique static IP address.

33. I then configured three computers with a Windows 7 operating system, and the fourth computer was a MacBook Pro configured with OS X El Capitan version 10.11.4. I installed a different BitTorrent client[2] onto each computer system as listed below:

[1] An IP address is a numerical value assigned to a computer or device that transmits and receives data via the Internet. When a computer user accesses the Internet, their Internet Service Provider assigns them a unique IP address for that session. In order to identify a computer user who is downloading files via the Internet, one must be able to identify the IP address the user was using at that exact time and date of downloading.

[2] A BitTorrent client is software that enables the BitTorrent protocol to work.

Computer	Operating System	BitTorrent Client
Dell Laptop	Windows 7	uTorrent Version 3.4.7
Dell Laptop	Windows 7	qBittorrent Version 3.3.4
Dell Laptop	Windows 7	Transmission Version 2.84
MacBook Pro Laptop	OS X El Capitan 10.11.4	uTorrent Version 1.8.7

34. After installing the BitTorrent clients, I also installed Wireshark and WinDump onto each computer. Wireshark and WinDump are programs that capture network traffic and create PCAP files. PCAP stands for "packet capture." PCAPs are akin to videotapes. Indeed, a PCAP is like a video recording of all the incoming and outgoing transactions of a computer. I have used Wireshark and WinDump software while in law enforcement to examine network traffic while investigating P2P cases.

35. After installing Wireshark and WinDump onto each of the computers, I transferred the movie files that I created for the test to each of the four computers.

36. I then used one of the BitTorrent clients on the test computers to make .torrent files. I then seeded the four test movies.

37. On June 3, 2016 the test was conducted. Given only the torrent files, IPP was able to correctly identify all four static IP addresses for each of the test computers that were seeding the movies within minutes of starting the test. Soon after the test, IPP sent me the PCAP files they recorded during the test for each one of my static IP addresses.

38. I reviewed IPP's PCAPs vis-à-vis the PCAP log files created by each of my test computers, and determined that IPP's PCAPs match my PCAPs. This could not have happened unless IPP's server was connected to the test computers because the transactions would not match.

39. I also conducted an examination of IPP's PCAPs to determine if the detection software can accurately identify the BitTorrent clients I used during the test. Using Wireshark

software I loaded IPP's PCAPs recorded on the day of the test. IPP's system was able to accurately record the names and version numbers of all four BitTorrent client's software I used on each of the test computers.

40. When a BitTorrent client is installed onto a computer, the computer randomly selects a port number for its network communication. A port number is an integer ranging from 0 to 65535. The following is a chart listing the port number assigned to each of the test computers:

Computer	BitTorrent Client	Port
Dell Laptop	uTorrent Version 3.4.7	51892
Dell Laptop	qBittorrent Version 3.3.4	8999
Dell Laptop	Transmission Version 2.84	51413
MacBook Pro Laptop	uTorrent Version 1.8.7	10088

41. Examination of IPP's PCAP revealed that the port numbers recorded by IPP's system matched the port numbers from the test computers used for BitTorrent communications. Accordingly, my analysis confirmed that IPP was able to accurately identify the port number assigned to each test computer's BitTorrent client.

42. From this test, I concluded that IPP's infringement detection system worked, and had a subpoena been issued for my IP addresses, it would have revealed my identity. I also concluded that IPP's infringement detection system accurately identifies the BitTorrent clients as well as the BitTorrent client's port number.

43. In the past, Malibu has also retained Excipio GmbH's ("Excipio") to track infringement of Malibu's copyrighted works. In June 2013, in anticipation of the Bellwether trial in the Eastern District of Pennsylvania, I conducted a test of Excipio's infringement detection system. After performing the test, I concluded that Excipio's infringement detection system works. Specifically, the system accurately records the IP address of a person using

BitTorrent to transmit data to Excipio's computer servers. Excipio's system operates nearly the same fashion as IPP's system.

44. In addition to testing Malibu's investigators' systems, I have also conducted computer forensic examinations for Malibu in their copyright infringement cases throughout the country.

45. Indeed, in my role as an expert for Plaintiff, I have examined countless computer hard drives for evidence of: (a) the use of BitTorrent; (b) infringement of the copyrighted "X-Art" works owned by Plaintiff; (c) spoliation of evidence; and (d) suppression of evidence. These examinations have revealed either: (1) evidence of copyright infringement of Malibu Media, LLC's works; or (2) evidence of suppression and spoliation. Sometimes I have found both. By way of illustration, below are examples where Malibu obtained a Defendant's hard drive and discovered evidence of its movies, spoliation, and/or defendants' failures to disclose all hard drives.

a. *Malibu Media, LLC v. Weaver*, No. 8:14-cv-01580-VMC-TBM (M.D. Fla. 2015): In *Weaver*, the Court ordered production of the hard drives, and my forensic examination revealed evidence which irrefutably demonstrated: (a) Defendant's BitTorrent use; (b) the prior existence of numerous X-Art titles; (c) the deletion of BitTorrent files and uninstallation of a BitTorrent client; and (d) the existence of other computer devices that have not been produced. Because of this examination, Malibu was able to successfully disprove Defendant's denial of infringement.

b. *Malibu Media, LLC v. Huseman*, No. 1:13-cv-02695-WYD-MEH (D. Colo. 2014): In the *Huseman* case, I discovered evidence of: (a) BitTorrent use; (b) the prior existence of numerous X-Art titles; (c) the deletion of BitTorrent files and uninstallation of a BitTorrent client; and (d) the existence of other computer devices that had not been produced to me for examination, one of which *contained* titles of Plaintiff's copyrighted works. Ultimately, the parties stipulated to a final judgment in favor of Malibu Media, LLC.

c. *Malibu Media, LLC v. John Doe*, No. 1:14-cv-10155-KBF (S.D.N.Y. 2015): My forensic examination revealed that defendant had over eleven different file destruction software programs on his hard drive – each with the capability of destroying substantial amounts of data. He used several of the software programs just days before turning it over for imaging and examination. I also detected that prior to defendant's use of the file destruction software, the defendant connected another undisclosed external storage device to his hard drive. This suggested that defendant was storing data which he wanted to retain prior to using the file destruction software programs on his hard drive. Ultimately, the defendant admitted to his infringement and apologized to Malibu.

d. *Malibu Media, LLC v. Tashiro*, No. 1:13-cv-00205-WTL-MJD (S.D. Ind. 2014): My examination revealed that defendants deleted thousands of BitTorrent files the night before producing the hard drives for imaging. My examination also revealed that defendants possessed and used other hard drives which were never disclosed or produced during discovery. Ultimately, the court imposed terminating sanctions against defendants for failure to disclose documents, spoliation, and perjury.

e. *Malibu Media, LLC v. John Doe*, No. 12-2078 (E.D. Pa. 2013):. In this "Bellwether" case, my examination of defendant's hard drive revealed that he installed a Windows operating system three (3) days after being served with a subpoena for production of his computer device. This installation resulted in the complete destruction of all files contained within the hard drive prior to the Windows installation. After falsely testifying, Defendant admitted that he had downloaded Plaintiff's copyrighted works and had wiped his desktop computer (by installing a new Windows operating system) to conceal the infringements. In the end, the Court entered a substantial judgment in favor of Malibu.

46. I am paid on an hourly basis by Malibu Media, LLC, at the rate of $325.00 per hour for pre-trial investigative work, although the fee increases if I am required to testify at trial.

FURTHER DECLARANT SAYETH NAUGHT.

DECLARATION

PURSUANT TO 28 U.S.C. § 1746, I hereby declare under penalty of perjury that the foregoing is true and correct.

Executed on this 19th day of August, 2016.

By:_________________________
PATRICK PAIGE

Exhibit 7

Declaration of Stephen M. Bunting, S3H (217-cv-01731)_000155, dated 12/11/18

DECLARATION OF STEPHEN M. BUNTING

I, STEPHEN M. BUNTING, DO HEREBY DECLARE:

1. My name is Stephen Michael Bunting. I am over the age of twenty-one (21), and I am competent to make this Declaration. I make this Declaration voluntarily and the facts stated herein are based on my personal knowledge and information.

2. Attached hereto as Exhibit "A" is a true and accurate copy of my Curriculum Vitae which truly and accurately represents my relevant employment history, training, experience, certifications, and expert-witness experience.

3. I currently work as Director of Services for SUMURI, LLC and as independent forensic consultant as owner of Bunting Digital Forensics, LLC. Prior to that, I was a police officer from 1980 until 2009 with the University of Delaware Police from which I retired as a Captain. During the last ten years with the University of Delaware Police, I was in charge of the digital forensics and cyber investigations unit, that I founded. From 2009 until early 2013, I was a Senior Forensic Consultant with Forward Discovery, LLC, which in late 2012 was acquired by Alvarez and Marsal (NY) where I was a manager in the digital forensics division. I founded Bunting Digital Forensics, LLC in early 2013.

4. I have taken hundreds of hours of training in digital forensics, network forensics, and cyber investigations. I have provided training in the same topic areas, from beginner to expert levels, to members of various local, state, and federal law enforcement agencies and private sector examiners. I have trained like personnel internationally in over twenty-one (21) different countries. I have provided training, as either a part-time employee or contractor, for Guidance Software, Magnet Forensics, MicroSystemation, A.B., Organization of American States, and the

U.S. Department of State Anti-Terrorism Assistance Program (Cyber Division). I have developed digital forensic or cyber training programs for several government and private entities.

5. I hold several industry-related certifications. I was the recipient of the 2002 Guidance Software Certified Examiner Award of Excellence for receiving the test score on my certification examinations. Among my varied certifications I am an EnCase Certified Examiner EnCE (Guidance Software), an AccessData Certified Examiner (ACE), Certified Computer Forensics Technician (HTCN), and a Certified XRY Instructor.

6. I am the principle author of *EnCase Computer Forensics - The Official EnCE: EnCase Certified Examiner Study Guide, 3rd Edition,* the co-author of *Mastering Windows Network Forensics and Investigation, the author of EnCase Computer Forensics—The Official EnCE: EnCase Certified Examiner Study Guide, 2nd Edition*, and the co-author of *Mastering Windows Network Forensics and Investigation 2nd Edition, the author of EnCase Computer Forensics—The Official EnCE: EnCase Certified Examiner Study Guide, 3rd Edition* (all published by Wiley).

7. I have written numerous articles in the field of digital forensics over my career. Most recently, I published two articles regarding spoliation examinations in which several peer-to- peer cases on which I have consulted were referenced in a hypothetical context: *Forensic Analysis of Spoliation and Other Discovery Violations - Part 2 of a 2-Part Series - Windows Examinations* - eForensics Magazine - December 2016 *Forensic Analysis of Spoliation and Other Discovery Violations - Part 1 of 2-Part Series - Macintosh Examinations* - eForensics Magazine - October 2016

8. I have testified as a fact and expert witness numerous times in the field of computer forensics before state and federal courts in Delaware and New Jersey. I have submitted affidavits,

as an expert in digital forensics, on many matters in several states, including Delaware, Georgia, and South Carolina.

9. No court has ever refused nor has any attorney ever challenged to accept my testimony on the basis that I was not an expert or not qualified in the field of computer forensics.

10. As a digital forensics examiner I have acquired and examined hundreds of computer systems and mobile devices for various local, state, and federal agencies, in addition to scores of private clients. The types of cases or examinations include: homicide, child-exploitation, fraud, Medicaid fraud, unlawful intrusion into computer systems (hacking), intellectual property theft, research fraud, email forgery, criminal impersonation, forgery, sexual harassment, peer-to-peer, and spoliation. I have acquired computer systems of many types, including servers, virtual servers, desktops, and laptops. I have acquired hundreds of mobile devices (feature phones and smart phones), both logically and physically. I also have acquired smart phones using JTAG and chip-off techniques, both of which require disassembly and working with the printed circuit boards inside a smart phone.

11. I have considerable experience with network-related cases, such as unlawful intrusions and peer-to-peer cases. I have investigated or provided digital forensics support to several unlawful intrusion incidents in both a law enforcement and a private sector capacity.

12. In the past, I have consulted with Computer Forensics, LLC, in copyright infringement cases utilizing IPP's technology. I'm familiar with the technology that was used in those cases to detect the copyright infringement offenders.

13. As a police officer I received specialized training in conducting peer-to-peer investigations by S.A. Flint Waters with the Wyoming Internet Crimes Against Children (ICAC) Task Force. S.A. Waters developed the Wyoming Toolkit, a customized version of Phex, a peer-

to-peer client on the Gnutella network. I participated with members of the State of Delaware ICAC in this training program and afterwards in a task force conducting peer-to-peer investigations. Using the Wyoming Toolkit, we searched for child sexual exploitation images and movies on the peer-to-peer networks. When images were found, the software identified offending computers by their IP addresses.[1] The IP addresses hosting the illegal images are parsed by the toolkit using an IP geolocation database by which offending IP's are isolated or filtered to only those within our police jurisdiction. Once offending IP's were found in Delaware, we would request that the Attorney General's office submit subpoenas to the ISP (Internet Service Provider) for specific customer information and address of the offending IP address. As IP addresses are often time-specific, we submitted the exact date / time (along with time zone offset) for the offending IP address. The ISP would return to us the customer or subscriber information (name, address, account information, etc.) for the ISP in question. We would investigate further and obtain a search warrant for the premises at which the IP was hosted. The search warrant would permit us to seize all media and electronic devices capable of holding digital media, as we did not know specifically which device behind the router was the offending device. The IP address detected by the peer-to-

[1] A public or internet routable IP address is a router or computer's address on the internet at a specific time. IP addresses uniquely identify a computer, as no two computers can have the same exact public, internet routable, IP address at the same time. If the address is that of a router, the computer typically has a private address behind the router. In a typical home network, the ISP provides a 'box,' which is often both a modem and a router / firewall / DHCP server. The router has a public or internet facing IP address assigned to it. On the back side of the router, several devices (computers, smart phones, etc.) are connected using private addresses. Thus, several devices in a home network share the public internet routable address assigned to the ISP's box (router). Other computers on the internet, including peer- to-peer software, see and use the public facing IP address assigned to the customer's router. The router routes network traffic for specific devices on the private side or behind the router using a protocol called NAT (Network Address Translation), thus assuring network traffic is sent to the correct computer. IP addresses, as mentioned, are often time specific. These IP addresses are called dynamic IP addresses. They are assigned for certain periods of time, called leases. There is great variability in how often dynamic IP addresses change, but because they can and do change, the specific time of the offense is necessary to determine which subscriber was assigned a specific IP address at a specific time. ISP's maintain connection logs that record to whom a specific IP address is assigned and exactly when. By contrast, an IP address can be a fixed IP address. Even they can change and, as an investigator, you do not know which type a subscriber has and thus the exact time is always obtained and submitted to an ISP when requesting subscriber information.

peer software was the public facing internet addressable IP address of the router, which is associated with the subscriber and their residence and not to a specific computer in the residence. Because it was a criminal investigation, we requested that the subscriber not be notified of the subpoena so that digital evidence would not be destroyed. Thus, in nearly all cases, the offending subscribers were surprised by the execution of the search warrant. In all the times that we did so, not once did the IP address lead to an innocent person's residence. Rather, we always found evidence therein of child sexual exploitation media on the computer system(s) therein.

14. I have found that the Wyoming Toolkit was a most reliable tool for identifying the IP addresses for peer-to-peer clients that were hosting child sexual exploiting images and video.

15. Most recently, I tested the infringement detection software by a company called MaverickEye UB (MEU). This software and hardware platform is owned and run by GuardaLey, LTD ("GuardaLey"), a German company located in Eggenstein, Germany. It is my understanding that GuardaLey's system is substantially similar to another German company called IPP International UG ("IPP").

16. I constructed and then conducted a test to determine the accuracy of the GuardaLey's system as to its ability to detect an infringing party's IP address, identifying metadata (client software and version used by infringer), and identifying the known test files distributed on the torrent network. The manner in which GuardaLey's system works and the manner in which the software that I have used in my law enforcement capacity (Wyoming Toolkit) work to connect a peer-to- peer violation with an IP and subsequently with a subscriber are quite similar. In fact, in my opinion, GuardaLey's system is much better with greater integrity features. Further, my test confirmed that GuardaLey's system is accurate. My report illustrating this conclusion is attached hereto as Exhibit "B."

17. I have been retained by Strike 3 Holdings, LLC to provide digital forensic services and consulting in matters of copyright infringement. I am paid on an hourly basis by Strike 3 Holdings, LLC at the rate of $250 / hour for my digital forensics services.

18. I have read through the Honorable Judge Royce C. Lamberth's Memorandum Opinion ("DC Opinion") in the matter *Strike 3 Holdings, LLC v. John Doe subscriber assigned IP address 73.180.154.14*, No. CV 18-1425, (D.D.C. Nov. 16, 2018). The instant declaration specifically addresses the portion of the DC Opinion discussing the technology behind Strike 3 Holdings' case. And more specifically, the portion of the DC Opinion which states:

> Since Bittorrent masks users' identities, Strike 3 can only identify an infringing Internet protocol (IP) address, using geolocation technology to trace that address to a jurisdiction. This method is famously flawed: virtual private networks and onion routing spoof IP addresses (for good and ill); routers and other devices are unsecured; malware cracks passwords and opens backdoors; multiple people (family, roommates, guests, neighbors, etc.) share the same IP address; a geolocation service might randomly assign addresses to some general location if it cannot more specifically identify another.

STRIKE 3 HOLDINGS, LLC, Plaintiff, v. JOHN DOE subscriber assigned IP address 73.180.154.14, Defendant., No. CV 18-1425, 2018 WL 6027046, at *1 (D.D.C. Nov. 16, 2018).

19. Below, I address each of the foregoing issues in turn.

Virtual Private Networks and Onion Routing Spoofing of IP Addresses

20. Often times, in cases involving cybercrimes and IP addresses, defendants claim that their IP address was "spoofed." However, in cases involving detection systems that connect to peers using a TCP/IP connection, such as the Wyoming Toolkit, GuardaLey's system, or IPP's system, spoofing cannot be accomplished.

21. IP spoofing is typically used in DDOS (denial of service) attacks. Indeed, specially crafted network packets can be used to create denial of service attacks, but these packets are small and usually involve repeatedly sending the same small crafted packet over and over again, creating

a flood of messages that results in a denial of service attack. Creating a few small, specially crafted packets that are sent repeatedly is a completely different task than trying to do so for a BitTorrent stream, where tens of thousands of packets, mostly all of which are different, are involved.

22. With respect to spoofing in the BitTorrent context, in a practical sense, a very technically adept person would have to know a victim's IP address. This person would have to physically connect a computer into the same network segment as the intended victim in order to intercept the network traffic involved. Doing so would involve considerable knowledge and skills, in and of itself, and could involve illegal access to a building or ISP network equipment. The person would need to have the file in question on their computer, be sharing it using BitTorrent software, and have some software or code capable of or rewriting tens of thousands of BitTorrent packets on the fly, as any delay could cause a time-out. While many things are theoretically possible, I am unaware of any such software being available. Such an endeavor would involve tremendous effort and resources. In addition, the person would have to know that a particular file was being monitored for copyright infringement downloading. And finally, such a person would have to have a very strong motivation to undertake such a task and to target a particular person and/or IP address. Considering all that would be involved in such an endeavor, it is so unlikely to occur as to be nearly impossible.

23. Often IP spoofing, as described above, is interpreted or confused by many, including Google's search engine, with IP address hiding. If you search for "IP spoofing software," you will find most of the search results will involve VPN (Virtual Private Network) software. VPN software allows the user of a computer to create an encrypted tunnel to a VPN server from which the internet traffic emerges unencrypted, provided of course it was unencrypted to begin with. The VPN server's internet facing IP address becomes the user's public internet-

routable IP address. It acts as a proxy and becomes the user's frontend IP address on the internet. VPN's are intended for privacy of a user's internet traffic and also for protecting the identity of a user's true IP address (the IP address which their ISP has assigned to them). If an infringer uses a VPN to engage in BitTorrent file sharing, other peers within the swarm will be able to identify the infringer by the infringer's public facing internet routable IP address which would the VPN's IP address. In other words, when a VPN is being used, other peers can only trace the connection to the front-end or public-facing, internet routable IP address – which would be the VPN IP address. To obtain the true IP address of the user behind the VPN, one would have to contact the VPN owner or manager. If the VPN owner maintain logs, and many intentionally do not, the connection to the source can then be identified through the subpoena process.

24. In the past, I actually conducted a test on this exact VPN issue. Indeed, earlier this year, when I tested Guardaley's system, I also tested this VPN theory. To do so, I configured one test laptop (MacBook Pro – High Sierra) with a VPN service. With the VPN enabled, I launched Transmission (a popular BitTorrent client) and shared four separate test files. I noted the public, internet-routable, frontend VPN IP address in use by the test laptop. After running this BitTorrent configuration overnight using the VPN service, GuardaLey reported to me that their system captured and downloaded the test files from the IP address that I had recorded for the test laptop. It was, as expected, the IP address of the VPN server. Thus, a test of the scenario, establishes that the VPN IP address, and not my true ISP's IP address was being made public via the BitTorrent network.

Unsecured Routers and Other Devices

25. The DC Opinion also lists concerns about unsecured routers and devices.

26. During my time at Bunting Digital Forensics, LLC, I was involved in a case where the owner of the computer and charged party was professing his innocence, claiming someone else must have used his wireless network, citing a neighbor who reportedly engages in photography of a questionable nature. However, the evidence on his computer suggested otherwise. The software used by the investigators detected the name and version of the peer-to-peer software client involved, which happened to match the one found on his machine. Further, the same exact images detected by the investigative software were found on his machine. His claims were without merit and in direct contradiction to the overwhelming digital evidence found on his computer.

27. Unsecured wireless routers in homes used to be commonplace 15 years ago. In recent years, however, Internet Service Providers (ISP's) have undertaken great effort to provide and deploy secured wireless systems. Most "internet interface boxes" (combination modem / router / firewall / DHCP server) which are rented to subscribers are preconfigured to operate with WPA2 security with a complex password already set. These devices are secure out of the box with strong encryption and complex passwords that are lengthy alpha numeric passphrases. Thus, valid claims of compromised home wireless systems today are, in my experience, rare compared to 15 years ago.

Malware Cracks Passwords and Open Backdoors

28. The DC Opinion states, that "malware cracks passwords and opens backdoors." However, I have never heard of or encountered malware which accesses a user's computer, automatically downloads and installs a BitTorrent client, and then proceeds to download .torrent files correlating to several of Plaintiff's works over the course of several months.

Multiple People Share the Same IP Address

29. Although there may be several household members who access the internet with the same router, learning the identity of the subscriber to an IP address user in connection with commission of a crime is instrumental, necessary, and the only means of learning the perpetrator's true identity – even if the subscriber is not the perpetrator.

30. And, in my experience, the IP address's subscriber, or a family member thereof, is likely the offending party.

Geolocation Technology

31. Lastly, the DC Opinion states, "a geolocation service might randomly assign addresses to some general location if it cannot more specifically identify another."

32. Geolocation services are used to approximate locations of IP addresses. Such geolocation services are often used as a tool in e-commerce fraud prevention measures. Further, the Wyoming Tool Kit that I used as a law enforcement officer to identify offenders distributing sexual exploitive images of children using peer-to-peer software, used commercial geolocation services to obtain the approximate location of IP addresses for purposes of assigning IP addresses to various law enforcement jurisdictions. Geolocation databases are not used to determining the exact address of a subscriber of an IP address for purposes of executing a search warrant. Rather, to determine an IP address subscriber's physical address on which to execute a search warrant, law enforcement relies on a subpoena that is served upon the ISP. When law enforcement uses this technology and methodology to identify and arrest those creating and exchanging sexually exploitive images of children, they are applauded for their efforts. Similarly, Strike 3 Holdings, LLC uses geolocation services to determine an approximate location of an IP address so as to identify a court with jurisdiction in that region. Once that court issues a subpoena, the exact name

and specific physical address of the party responsible for the offending IP is identified. Strike 3 Holdings, LLC is, thus, using a process very much like that used by law enforcement.

FURTHER DECLARANT SAYETH NAUGHT

DECLARATION

PURSUANT TO 28 U.S.C SS 1746, I hereby declare under penalty of perjury that the foregoing is true and correct.

Executed December 11, 2018.

Stephen M. Bunting

Exhibit 8

Declaration of Brandon Garcia-Paeth in Support of Defendant's Opposition to Plaintiff's Motion for Summary Judgment, Case no. 2:17-cv-01731-TSZ, 02/25/2019

Honorable Thomas S. Zilly

UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF WASHINGTON

AT SEATTLE

STRIKE 3 HOLDINGS, LLC, a Delaware corporation, Plaintiff, vs. JOHN DOE subscriber assigned IP address 73.225.38.130, Defendant.	Case Number: 2:17-cv-01731-TSZ **EXPERT REPORT OF BRANDON GARCIA-PAETH**

Summary

I am Brandon Garcia-Paeth, an independent consultant. I have expertise in packet capture and protocol analysis.

Objective

I have been retained by the defendant's council in case 2:17-cv-01731-TSZ for the purpose of providing expert testimony regarding the details of the packet captures provided by the plaintiff. I am being paid $100 per hour for analysis and testimony.

Qualifications

From 2009 to current I have worked as a Network Engineer for a software development company. My duties include packet capture analysis with a focus on protocol specific communications. As part of my duties I use on a daily basis for network analysis.

Prior to my current employment I used tcpdump, ethereal, and wireshark for packet analysis and troubleshooting various network and protocol level issues. I am familiar with the popular bittorrent clients as well.

Also included is my condensed resume.

Material Reviewed

001 - DIS 1.002 -Complaint.pdf
001-2 - DIS 1.002 -Report on Copyrights.pdf
043 - DIS 1.002 - Amended Complaint.pdf
043-1 - DIS 1.002 - Amended Complaint - Ex A.pdf
107 .torrent file
484 .pcap files

Terminology

Torrent client – an application which uses the bittorrent protocol.

.torrent file – file which represents a torrent container.

Torrent – a container that can hold any form of data such as video, audio, or text.

Torrent piece – Torrents are made up of torrent pieces. Each torrent piece is represented by a hash value that is checked when downloaded. If the hash is incorrect then the piece is redownloaded.

Data block – the smallest addressable component of a torrent piece. A data block is 16KB of data.

PCAP – PCAP is short for packet capture and is considered an industry standard for storing network captures.

Summary of opinions

From the amended complaint there are 87 total works listed with 405 of the 484 provided packet captures are associated with a listed work. Also, of the 87 listed works 10 had no packet captures associated with them. 11 of the works had greater than 10 packet captures associated. The largest number of pcaps for an associated work is 26.

From the provided packet captures only one for each work listed was analyzed. The packet capture analyzed was the most recent out of the packet captures provided that matched the hash for the listed work.

My analysis of the data shows that in each pcap only a very small percentage of the file was downloaded. One or two torrent pieces (16KB each) was downloaded in most cases. In a few of the pcaps no piece download was shown.

Of note on the provided pcaps is that they of communication from multiple internal IP addresses to IP address 73.225.38.130.

March 15, 2019

Date

Brandon Garcia-Paeth

Brandon Garcia-Paeth
16870 NW Sellers Rd
Banks, OR 97106

(971) 409-3332
garcia.paeth@gmail.com

OBJECTIVE

To obtain a position where the computer skills gained from my education and personal experience as well as my experiences in computer networking and systems administration can further the goals of the business.

SKILLS – TECHNICAL

- Windows 7, 8, 10
- Windows Server 2008, 2012, 2016
- Basic Linux Configuration and Administration
- Microsoft Exchange 2010, 2013
- Microsoft Office O365 Administration
- Network Protocol Level Troubleshooting
- Internet Information Services 7, 8
- Intermediate Firewall configuration
- Active Directory Configuration/Support
- Basic Scripting/Programming
- PC Software Setup/Maintenance
- PC Hardware Configuration/Installation
- Network Planning and Installation
- Cisco Routers and Switches
- TCP/IP and Subnetting

SKILLS – INTERPERSONAL

- Management and Team Statistics
- Team Planning and Communication
- Handling of Escalated Issues
- Accurate Equipment Documentation
- Training of Small Teams of Employees
- Excellent Written/Verbal Communication

EDUCATION

ITT Technical Institute - **(Cumulative GPA: 4.0 Perfect Attendance)**
Associate of Applied Science Degree in IT - Computer Network Systems
Portland, OR
Completed 06/09

EMPLOYMENT HISTORY

FaxBack, Inc.
Network Engineer
10/09 – Present
Maintain and administer company network including software and hardware. Troubleshoot network level problems with SIP, HTTP, and SMTP protocols as well as others. Design, configure, and implement network components for network expansion. Monitor network performance.

Pacific Office Automation
Delivery Driver
Beaverton, OR
10/05 – 06/07
Delivered copiers and fax machines to customer locations. Assisted with copier-specific network setup. Maintained accurate delivery logs of all equipment being delivered and being returned company premises. Assist with network configuration of networked copiers.

Work	Hash	Site	UTC	Published
1	1BC8C1ADCAA75C3EC9408C8CCBF5147863205E6C	Tushy	9/5/2017 10:40	9/3/2017
2	0326E8923C58B52725F5A7857833A4CD3E715289	Tushy	5/15/2017 4:40	5/6/2017
3	039F4779148D3E374D990283A83AC46A0219DAE9	Vixen	5/12/2017 6:25	4/19/2017
4	0CAB7415EAE003A2C3835DE5FC716759A49040B9	Tushy	7/5/2017 19:58	7/5/2017
5	0CDEB18021838E8E2A694A7D16D9A45366CFABB6	Blacked	8/8/2017 21:54	8/8/2017
6	1278F4C4BF0B45678418F6CC8F8844DE4AB68C83	Tushy	5/15/2017 5:03	4/26/2017
7	1487A26EAAAD70318258AB9F506506A8F293533A	Blacked	5/21/2017 18:02	5/5/2017
8	18A6F7D0E24D4FA3CC1589DE496D1AD9433CF09B	Blacked	6/20/2017 1:03	6/19/2017
9	1A032CB38BB2AF87DAF2B239A1A17B6C713EBC26	Blacked	8/12/2017 13:46	8/3/2017
10	1C2C06D480942F4FE7FDCED4759E93805E02B54B	Tushy	5/24/2017 1:49	5/21/2017
11	1D1B18BB0C921D6E1A6D148E4542257B42A2469F	Tushy	6/22/2017 8:52	6/20/2017
12	1D63168E762F9CB41AE4DBD6646599AD0EFF3911	Blacked	7/10/2017 20:05	7/9/2017
13	1D7E521CD7368013A7F1B28494A2AC43D8F99F0E	Vixen	9/3/2017 5:01	9/1/2017
14	1D7E721AC3B8D955BBCAD8D62F57AF030BD1F315	Vixen	6/6/2017 10:18	6/3/2017
15	22883186DAB5FCA92C8513AD939652BCB867FD5C	Tushy	8/21/2017 10:03	8/19/2017
16	22C377CC65B1695E6470BFAF967C4C825391EF90	Blacked	8/1/2017 8:09	7/29/2017
17	24D6E127081B069994E81CA544B8FF3E3A0A33D3	Tushy	5/17/2017 6:35	5/16/2017
18	258961E123E520633A96CDF11E8E6F60E233C816	Vixen	7/24/2017 17:24	7/23/2017
19	289FE7D65DFCFACB416832D12862105A2762841A	Blacked	5/12/2017 5:45	5/10/2017
20	31577E16E1B68BF13F30BE538E1BAF66E224726A	Tushy	8/1/2017 5:04	7/30/2017
21	322F6ABAB019761A6FF3C1211AF75B28137F013F	Vixen	6/9/2017 20:46	6/8/2017
22	34452073A3328CE2AF5FC73A5A8DDD4141E85B4A	Vixen	8/23/2017 10:51	8/22/2017
23	374A3B65D604113BB3880FDACE83FD1EFED3CA7C	Tushy	8/15/2017 12:51	8/14/2017
24	3945FEF635D609C3FB77DD4762FC2570E7E12D7C	Blacked	5/21/2017 16:45	5/20/2017
25	3F3D4931127C380DD0AA05C298E26438267560BB	Vixen	7/5/2017 4:23	6/28/2017
26	408577469D1675504E89F205C619738007D08DD9	Blacked	6/9/2017 20:59	6/9/2017
27	4125860EC76C1E0880F652DA94EB84D375A64436	Tushy	8/5/2017 12:02	8/4/2017
28	464AB452DA8258FA23BA74830F0D57EE7CA518C5	Tushy	8/26/2017 12:52	8/24/2017
29	48F5E3FE474EA76DE23D7D0A8F27ADA15F5C98D7	Blacked	7/20/2017 21:22	7/19/2017
30	4B86BC16D0E5A0983C578B61ED87BC62C55B116A	Vixen	8/14/2017 12:50	8/12/2017
31	4F0D3D0FD3F88791F4933080453A052BE6924F22	Tushy	10/12/2017 21:12	10/8/2017
32	4FAE423CFA8C54409A4658429D7CB2B3E0F2E8B1	Vixen	9/27/2017 2:20	9/11/2017
33	4FF62836FC3C509617EE5DE7658EAABE045C0BA1	Tushy	9/16/2017 16:46	9/13/2017

34	5003D85013A07470D85A3250EF4B3393B6E2CB04	Tushy	7/12/2017 20:00	7/10/2017
35	5176733783D1199D43060681D7AE2D4E3B5C9AF9	Blacked	7/19/2017 22:47	7/14/2017
36	53FF1B4BD8FB69630FE0A67611FE747F902F6874	Vixen	7/20/2017 21:17	7/18/2017
37	5A06B4EA4DB48984499F2E9EA7213220E835089D	Blacked	6/16/2017 14:31	6/14/2017
38	5AA7FC6E46AEF9EC1227A939EADB3351AD495F12	Vixen	8/8/2017 23:27	8/7/2017
39	5C208E2ABF6083135CA52776A02D87442F215D60	Tushy	6/19/2017 18:46	6/15/2017
40	5F25F5C8970A1123950D8543F0C954308ECC9D12	Tushy	9/24/2017 16:04	9/23/2017
41	6503CB2EAECE7FA2F1D71B98E41D6D845BF7B794	Vixen	8/18/2017 16:01	8/17/2017
42	6960957E412263AA671D4F7A15737527D71A7C08	Tushy	9/8/2017 22:40	9/8/2017
43	69AC2D8751ABF0FED5C443A1CE77A7C7529B7AC9	Vixen	5/10/2017 8:28	5/9/2017
44	6A53ECB874B094837053EB7B7142560F0A85A9C2	Vixen	9/22/2017 9:04	9/21/2017
45	6B9175E9708A1BE765BBDC6582A68A12E44A33E3	Vixen	7/14/2017 21:54	7/13/2017
46	72F519FE9EED3C466979E55CFEBF253309A8106C	Vixen	5/16/2017 12:11	5/14/2017
47	74C66B184CB3F25F69326EF0C5529CDB680A8C47	Vixen	5/25/2017 3:53	5/24/2017
48	792198F0F41E1FFA44A67E62F451EC11B9B692EF	Vixen	8/1/2017 8:35	7/28/2017
49	7E4981D21DDD4B8D9EB5905B1B8A95461915A160	Blacked	8/24/2017 11:53	8/23/2017
50	82EC6E9F2A9287FD59C2B571FDC0CDED7EDDBB81	Blacked	7/5/2017 4:24	6/29/2017
51	8519F3BB18D38EB8472CD07987B1BC2224E7EC22	Vixen	11/9/2017 8:28	10/11/2017
52	88D30B83D9E749F514380A5F2E9C3E876CF55431	Tushy	8/10/2017 10:01	8/9/2017
53	8D906EA439B8BF052A8D68240F71C6D9ACE1E17A	Vixen	7/5/2017 15:34	7/3/2017
54	8F55C47AC0C8FED6F30E2C094965B3CF4749FA41	Vixen	9/20/2017 9:40	8/27/2017
55	921AED6337A58B159CFAF9DADDFE2D91CDFF8AB3	Tushy	8/12/2017 11:16	6/25/2017
56	94E00EDACF46F8763B4B28A29BEB83473AC2BA8E	Blacked	11/22/2017 11:18	11/21/2017
57	9B5E94F7A0C627798E8020DFAA9A28609D1AB82A	Tushy	7/20/2017 21:27	7/20/2017
58	9C80B087C925D30BA01F72FC0EAABD8EAADF588A	Blacked	8/20/2017 9:20	8/18/2017
59	9D5513F0563852D9FB73EDC7D6318A6BB04334D9	Tushy	9/20/2017 11:43	9/18/2017
60	9E77DF7FCCB30D04DC6500C39CC3EF0AA2B48257	Blacked	9/6/2017 23:09	9/2/2017
61	ABC004062B9F9CF37E9A3A57F4BEA161154EECAE	Vixen	11/30/2017 20:59	9/26/2017
62	ABDFB02F5D20E29C32ABCE90A8478787DDA3C11D	Tushy	6/12/2017 17:58	6/10/2017
63	AE6A89DD0FB4978EAC561028F9FB06AA0A8D7E6A	Tushy	5/10/2017 9:29	5/1/2017
64	AFA4C44023577E2A90E1CFA8DB69A6F5D035B1D2	Blacked	9/8/2017 22:15	9/7/2017
65	B2EC2056C7699F25A118F23E36BB74FC7D3B7131	Vixen	7/9/2017 14:25	7/8/2017
66	B80F62F292E7B77184DC0BCF80ECE23CF7B23D15	Tushy	9/29/2017 10:28	9/28/2017
67	BA56E328AE2DBA8A20B327451656293E37FDAE35	Blacked	5/16/2017 12:04	5/15/2017

68	C496C2BFE4C6D994F43DC665F2CBEE16FE85777A	Tushy	6/6/2017 10:39	6/5/2017
69	C59734C1DC4D87F563ABE2D6E371C12FD12FC7D9	Blacked	11/2/2017 9:05	10/22/2017
70	C6965A70345AC1C86DD34737BF381734CA301655	Vixen	12/1/2017 12:28	10/1/2017
71	D2B9C8834073E3BF4B55F7BF45C7EA7BE5903569	Blacked	5/31/2017 11:36	5/30/2017
72	DB6040CB19308F376554AC18F5C883139311322D	Blacked	11/7/2017 1:43	9/17/2017
73	DCE0631B0833B899B8A4C577203A87AD00BD2B8B	Blacked	11/13/2017 1:30	11/11/2017
74	DCE1E033042DA8E7CFC7CEC42B7D21201BEDFD57	Tushy	7/5/2017 13:13	6/30/2017
75	E132114F31A37161B83D12BCE6320B65DE025C9B	Vixen	6/20/2017 1:02	6/18/2017
76	E1C14843DC58F3CB2CCB7383B242E4EE8D32363B	Tushy	8/1/2017 0:20	7/25/2017
77	E272AF63D15A4277BF857E93B225717C76F3DA9D	Tushy	5/15/2017 7:43	5/11/2017
78	E4BB4B0185636612E25A2955F474B4494789F63C	Blacked	10/12/2017 23:51	10/7/2017
79	E69BB37CE99BE570CC9EB659F45DDEF6E740E3BE	Blacked	8/14/2017 12:40	8/13/2017
80	E8910563DE2084C48C6A8C5801457339745A09FA	Vixen	5/31/2017 11:21	5/29/2017
81	EC31FAD9EF2492EACCD767B4A6E207BBF2765F0E	Blacked	9/13/2017 14:24	9/12/2017
82	F1132ADEB75DD2EA99B249DD70902C74E9DA7884	Tushy	9/3/2017 5:00	8/29/2017
83	F28E401CBB99CFB32E0808B7662BC50A9C5F64AD	Blacked	11/10/2017 0:59	9/22/2017
84	F8A92532C263D3E3497FF27A3FE569FF7BF15E37	Blacked	5/15/2017 6:09	4/25/2017
85	F8FEB2EE6C17B37610C5B2AE85F0266CB0C5C5BD	Blacked	7/5/2017 15:25	7/4/2017
86	FF7A5EE06C927438A3CAABC69D774D9CEACA8B9F	Tushy	7/17/2017 19:52	7/15/2017
87	FFD7D4C0A301487B3A11CBF1B3FC16410D42AEA0	Vixen	9/6/2017 23:08	9/6/2017

CRO App. FileDate	CRO Number	torrent file name	pcap count	mp4/mov size (byte)	pcap(s) analyzed
9/10/2017	PA0002052851	S3H (217-cv-01731)_000289.torrent	1	367001600	3590461132
6/16/2017	PA0002069288	S3H (217-cv-01731)_000280.torrent	7	275418972.2	3172688471
6/16/2017	PA0002069291	S3H (217-cv-01731)_000281.torrent	4	393058713.6	3165696486
7/6/2017	PA0002041555	S3H (217-cv-01731)_000282.torrent	1	313356451.8	3335254668
8/18/2017	PA0002077679	S3H (217-cv-01731)_000283.torrent	1	318379130.9	3595590476
6/15/2017	PA0002037565	S3H (217-cv-01731)_000284.torrent	7	281710428.2	3172857957
6/15/2017	PA0002037591	S3H (217-cv-01731)_000285.torrent	2	321168343	3165759834
7/7/2017	PA0002070823	S3H (217-cv-01731)_000287.torrent	12	222434426.9	3307340910
8/17/2017	PA0002077671	S3H (217-cv-01731)_000288.torrent	5	271203696.6	3631998944
6/22/2017	PA0002039282	S3H (217-cv-01731)_000290.torrent	2	283566407.7	3179038555
7/7/2017	PA0002070816	S3H (217-cv-01731)_000291.torrent	3	331297587.2	3289600304
8/17/2017	PA0002077662	S3H (217-cv-01731)_000383.torrent	5	298969989.1	3421595956
9/15/2017	PA0002052845	S3H (217-cv-01731)_000292.torrent	3	269924433.9	3631198988
7/7/2017	PA0002070834	S3H (217-cv-01731)_000293.torrent	3	331769446.4	3262401238
10/10/2017	PA0002086140	S3H (217-cv-01731)_000294.torrent	1	280923996.2	3521499028
8/11/2017	PA0002046872	S3H (217-cv-01731)_000295.torrent	3	189016309.8	3597764812
6/22/2017	PA0002039300	S3H (217-cv-01731)_000296.torrent	5	338165760	3179026787
8/10/2017	PA0002046877	S3H (217-cv-01731)_000297.torrent	2	393037742.1	3407695252
6/22/2017	PA0002039285	S3H (217-cv-01731)_000384.torrent	4	221018849.3	3179637169
8/11/2017	PA0002075051	S3H (217-cv-01731)_000298.torrent	1	344855674.9	3437541938
7/7/2017	PA0002070832	S3H (217-cv-01731)_000299.torrent	10	411954053.1	3274565966
9/15/2017	PA0002052852	S3H (217-cv-01731)_000301.torrent	1	331591188.5	3530112662
8/17/2017	PA0002048391	S3H (217-cv-01731)_000302.torrent	2	316009349.1	3596238182
6/22/2017	PA0002039289	S3H (217-cv-01731)_000303.torrent	8	324691558.4	3180327177
7/7/2017	PA0002070828	S3H (217-cv-01731)_000304.torrent	26	225821327.4	3407623478
7/7/2017	PA0002070825	S3H (217-cv-01731)_000305.torrent	20	313796853.8	3606109496
8/17/2017	PA0002077666	S3H (217-cv-01731)_000306.torrent	6	322311290.9	3631532710
9/15/2017	PA0002052837	S3H (217-cv-01731)_000307.torrent	1	264849326.1	3543787762
8/11/2017	PA0002046876	S3H (217-cv-01731)_000308.torrent	1	282129858.6	3393286602
8/17/2017	PA0002048373	S3H (217-cv-01731)_000310.torrent	6	391831879.7	3645007042
10/19/2017	PA0002058298	S3H (217-cv-01731)_000311.torrent	1	387249602.6	3762013108
9/15/2017	PA0002052839	S3H (217-cv-01731)_000312.torrent	1	216121999.4	3688125046
10/10/2017	PA0002086153	S3H (217-cv-01731)_000314.torrent	2	318158929.9	3663770604

8/18/2017	PA0002077678	S3H (217-cv-01731)_000315.torrent	8	244276265	3579985698
8/11/2017	PA0002046878	S3H (217-cv-01731)_000316.torrent	2	203004313.6	3456604496
8/10/2017	PA0002046875	S3H (217-cv-01731)_000317.torrent	1	276006174.7	3393271824
7/7/2017	PA0002070824	S3H (217-cv-01731)_000318.torrent	14	311815045.1	3606115884
8/17/2017	PA0002077669	S3H (217-cv-01731)_000319.torrent	2	207135703	3792003459
7/7/2017	PA0002070815	S3H (217-cv-01731)_000320.torrent	1	329745694.7	3274840350
10/9/2017	PA0002086134	S3H (217-cv-01731)_000321.torrent	0	340913029.1	
10/10/2017	PA0002086150	S3H (217-cv-01731)_000323.torrent	4	221889167.4	3534636886
9/15/2017	PA0002052841	S3H (217-cv-01731)_000324.torrent	0	387847290.9	
6/22/2017	PA0002039298	S3H (217-cv-01731)_000325.torrent	5	359609139.2	3172021921
10/10/2017	PA0002086168	53H (217-cv-01731)_000326.torrent	5	341951119.4	3695222586
8/10/2017	PA0002046873	S3H (217-cv-01731)_000327.torrent	0	186740899.8	
6/22/2017	PA0002039297	S3H (217-cv-01731)_000328.torrent	8	364201902.1	3177778681
6/22/2017	PA0002039294	S3H (217-cv-01731)_000329.torrent	1	329840066.6	3178289701
8/10/2017	PA0002046871	S3H (217-cv-01731)_000331.torrent	1	316418293.8	3438076186
10/10/2017	PA0002086163	S3H (217-cv-01731)_000333.torrent	1	211319521.3	3595613086
7/7/2017	PA0002070821	53H (217-cv-01731)_000335.torrent	20	304852500.5	3597966512
10/19/2017	PA0002090452	S3H (217-cv-01731)_000336.torrent	1	298414243.8	3895834524
8/17/2017	PA0002077673	S3H (217-cv-01731)_000337.torrent	7	248638341.1	3504223506
7/7/2017	PA0002070827	S3H (217-cv-01731)_000338.torrent	2	296495349.8	3644483596
9/15/2017	PA0002052843	53H (217-cv-01731)_000385.torrent	0	371594362.9	
7/7/2017	PA0002070817	S3H (217-cv-01731)_000339.torrent	4	264849326.1	3631410502
1/4/2018	PA0002069353	S3H (217-cv-01731)_000340.torrent	1	232165212.2	3966197860
8/11/2017	PA0002046869	S3H (217-cv-01731)_000341.torrent	24	289459404.8	3657221868
10/10/2017	PA0002086146	S3H (217-cv-01731)_000342.torrent	0	258159411.2	
10/9/2017	PA0002086139	S3H (217-cv-01731)_000343.torrent	3	360364113.9	3696452498
9/15/2017	PA0002052847	S3H (217-cv-01731)_000345.torrent	2	307023052.8	3597468568
10/10/2017	PA0002085861	S3H (217-cv-01731)_000347.torrent	0	310357524.5	
7/7/2017	PA0002074096	S3H (217-cv-01731)_000348.torrent	6	269232373.8	3290128658
6/15/2017	PA0002037577	S3H (217-cv-01731)_000349.torrent	4	284898099.2	3172721947
9/15/2017	PA0002052840	S3H (217-cv-01731)_000350.torrent	0	299232133.1	
8/17/2017	PA0002077664	S3H (217-cv-01731)_000351.torrent	8	297879470.1	3645877492
10/10/2017	PA0002086160	S3H (217-cv-01731)_000352.torrent	2	273185505.3	3796958220
6/22/2017	PA0002039283	S3H (217-cv-01731)_000353.torrent	1	380391915.5	3146465426

7/7/2017	PA0002074097	S3H (217-cv-01731)_000355.torrent	6	351346360.3	3260706307
11/21/2017	PA0002063627	S3H (217-cv-01731)_000356.torrent	0	508454502.4	
10/10/2017	PA0002086155	S3H (217-cv-01731)_000357.torrent	1	344436244.5	4013596716
6/22/2017	PA0002039295	S3H (217-cv-01731)_000362.torrent	16	320958627.8	3291440222
10/10/2017	PA0002086174	S3H (217-cv-01731)_000363.torrent	5	202983342.1	3902668520
11/27/2017	PA0002098000	S3H (217-cv-01731)_000364.torrent	0	288893173.8	
7/7/2017	PA0002070818	S3H (217-cv-01731)_000365.torrent	12	325425561.6	3631547166
7/7/2017	PA0002070833	S3H (217-cv-01731)_000367.torrent	10	220117073.9	3329719076
8/11/2017	PA0002046870	S3H (217-cv-01731)_000368.torrent	3	364684247	3631458964
6/22/2017	PA0002039286	S3H (217-cv-01731)_000369.torrent	9	259512074.2	3174038267
10/19/2017	PA0002058300	S3H (217-cv-01731)_000370.torrent	0	344048271.4	
8/17/2017	PA0002077675	S3H (217-cv-01731)_000386.torrent	5	385309737	3597625990
6/22/2017	PA0002039292	S3H (217-cv-01731)_000372.torrent	3	359766425.6	3203557651
9/15/2017	PA0002052846	S3H (217-cv-01731)_000373.torrent	7	344048271.4	3694638548
10/10/2017	PA0002086144	S3H (217-cv-01731)_000374.torrent	7	380758917.1	3631566602
10/10/2017	PA0002057455	S3H (217-cv-01731)_000375.torrent	3	269536460.8	3903136390
6/15/2017	PA0002037576	S3H (217-cv-01731)_000379.torrent	13	286041047	3179684087
7/7/2017	PA0002070819	S3H (217-cv-01731)_000380.torrent	3	316764323.8	3597518220
8/11/2017	PA0002075050	S3H (217-cv-01731)_000381.torrent	6	235122196.5	3501189868
9/15/2017	PA0002052844	S3H (217-cv-01731)_000382.torrent	1	408630067.2	3597426214

Requested Piece	Requested Block(s)	Requested Block Length	Piece(s) Delivered	Total Block Size	Percentage
0x35	0x0, 0x4000	0x4000	2	32768	0.009%
0x39	0x0, 0x4000	0x4000	2	32768	0.012%
0x92	0x10000, 0x14000	0x4000	2	32768	0.008%
0x3b5	0x0, 0x4000	0x4000	1	16384	0.005%
0x17a	0x0, 0x4000	0x4000	2	32768	0.010%
0x41	0x0, 0x4000	0x4000	1	16384	0.006%
0x12e	0x8000, 0xc000	0x4000	2	32768	0.010%
0xd	0x0, 0x4000	0x4000	2	32768	0.015%
0x0	0x0, 0x4000	0x4000	1	16384	0.006%
0xe7	0x8000, 0xc000	0x4000	2	32768	0.012%
0x35f	0x0, 0x4000	0x4000	2	32768	0.010%
0xc	0x0, 0x4000	0x4000	2	32768	0.011%
0x18	0x0, 0x4000	0x4000	1	16384	0.006%
0x8a	0x0, 0x4000	0x4000	1	16384	0.005%
0x2e7	0x0, 0x4000	0x4000	1	16384	0.006%
0x84	0x0	0x4000	0	0	0.000%
0x173	0x0, 0x4000	0x4000	2	32768	0.010%
0x48	0x0, 0x4000	0x4000	1	16384	0.004%
0x43	0x0, 0x4000	0x4000	2	32768	0.015%
0x86	0x0, 0x4000	0x4000	1	16384	0.005%
0x3	0x0, 0x4000	0x4000	2	32768	0.008%
0x23b	0x0, 0x4000	0x4000	1	16384	0.005%
0x77	0x0, 0x4000	0x4000	2	32768	0.010%
0xa2	0x0, 0x4000	0x4000	1	16384	0.005%
0x205	0x0, 0x4000	0x4000	2	32768	0.015%
0x1f9	0x0, 0x4000	0x4000	1	16384	0.005%
0x21b	0x0, 0x4000	0x4000	2	32768	0.010%
0x248	0x0, 0x4000	0x4000	1	16384	0.006%
0x5b	0x0	0x4000	1	16384	0.006%
0x44	0x0, 0x4000	0x4000	2	32768	0.008%
0x205	0x0, 0x4000	0x4000	1	16384	0.004%
0x43	0x0, 0x4000	0x4000	1	16384	0.008%
0x4d	0x0, 0x4000	0x4000	1	16384	0.005%

0x2a9	0x0, 0x4000	0x4000	2	32768	0.013%
0x157	0x0, 0x4000	0x4000	2	32768	0.016%
0x174	0x0, 0x4000	0x4000	1	16384	0.006%
0xc7	0x0, 0x4000	0x4000	1	16384	0.005%
0x9d	0x0, 0x4000	0x4000	2	32768	0.016%
0x3fa	0x8000, 0xc000	0x4000	1	16384	0.005%
				0	0.000%
0x7	0x0, 0x4000	0x4000	2	32768	0.015%
				0	0.000%
0xf6	0x0, 0x4000	0x4000	1	16384	0.005%
0x6f	0x0, 0x4000	0x4000	1	16384	0.005%
				0	0.000%
0x3da	0x0, 0x4000	0x4000	1	16384	0.004%
0x4de	0x0, 0x4000	0x4000	1	16384	0.005%
0x20	0x0, 0x4000	0x4000	2	32768	0.010%
0x1a8	0x0, 0x4000	0x4000	1	16384	0.008%
0xd	0x0, 0x4000	0x4000	1	16384	0.005%
0x1b6	0x0, 0x4000	0x4000	1	16384	0.005%
0xe5	0x0, 0x4000	0x4000	1	16384	0.007%
0x40	0x0, 0x4000	0x4000	1	16384	0.006%
				0	0.000%
0x36d	0x0, 0x4000	0x4000	1	16384	0.006%
0x35b	0x0, 0x4000	0x4000	1	16384	0.007%
0x39f	0x0, 0x4000	0x4000	2	32768	0.011%
				0	0.000%
0x71	0x0, 0x4000	0x4000	2	32768	0.009%
0x21d	0x0	0x4000	1	16384	0.005%
				0	0.000%
0x137	0x0, 0x4000	0x4000	2	32768	0.012%
0x14d	0x10000, 0x14000	0x4000	1	16384	0.006%
				0	0.000%
0x204	0x0, 0x4000	0x4000	1	16384	0.006%
0x61	0x0, 0x4000	0x4000	2	32768	0.012%
0x2c0	0x18000, 0x1c000	0x4000	1	16384	0.004%

0x512	0x0, 0x4000	0x4000	1	16384	0.005%
				0	0.000%
0x1e5	0x0, 0x4000	0x4000	1	16384	0.005%
0x2a6	0x0, 0x4000	0x4000	1	16384	0.005%
0x9	0x0, 0x4000	0x4000	1	16384	0.008%
				0	0.000%
0x1f4	0x0, 0x4000	0x4000	1	16384	0.005%
0x19e	0x0, 0x4000	0x4000	1	16384	0.007%
0x20b	0x0, 0x4000	0x4000	2	32768	0.009%
0x33e	0x0, 0x4000	0x4000	1	16384	0.006%
				0	0.000%
0x22b	0x10000, 0x14000	0x4000	2	32768	0.009%
0x3da	0x0, 0x4000	0x4000	1	16384	0.005%
0x14	0x0, 0x4000	0x4000	2	32768	0.010%
0x75	0x0, 0x4000	0x4000	2	32768	0.009%
0x12	0x0, 0x4000	0x4000	1	16384	0.006%
0x106	0x8000, 0xc000	0x4000	1	16384	0.006%
0xa0	0x0, 0x4000	0x4000	1	16384	0.005%
0xc2	0x0, 0x4000	0x4000	1	16384	0.007%
0x45	0x8000, 0xc000	0x4000	2	32768	0.008%

CERTIFICATE OF SERVICE

I, J. Curtis Edmondson, hereby certify that on March 15, 2019, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the following:

Bryan J. Case, WSBA #41781
Email: bcase@foxrothschild.com
FOX ROTHSCHILD LLP (SEATTLE)
1001 Fourth Avenue, suite 4500
Seattle, Washington 98154
Telephone: (206) 624-3600

Lincoln D. Bandlow, *Admitted Pro Hac Vice*
Email: lbandlow@foxrothschild.com
FOX ROTHSCHILD LLP (LOS ANGELES)
10250 Constellation Blvd., Suite 900
Los Angeles, California 90067
Telephone: (310) 598-4150

Attorneys for Plaintiff Strike 3 Holdings LLC

By: /s/ J. Curtis Edmondson
J. Curtis Edmondson

Exhibit 9

Amended Expert Report:

Reliability Assessment of IPP Software, Kal Toth,

04/15/19

Amended Expert Report - Reliability Assessment of the IPP Software

April 15, 2019
Prepared by Dr. Kal Toth, P.Eng., Portland, OR 97205
For Mr. J. Curtis Edmondson, Law Offices of J. Curtis Edmondson, Hillsboro, OR 97124

ABSTRACT

Plaintiffs' experts have asserted that the IPP software (NARS) is 100% accurate and free of defects. In my experience, claiming that operational software is defect-free is not credible. Neither is asserting that a complex software-based system detects infringement flawlessly. In this report I systematically examine the reliability of the IPP software.

I understand that during discovery, in response to formal requests, no technical documents or software modules of any kind specifying the IPP software were disclosed. This means that there exists no objective evidence that can be relied on to prove that the IPP software executes correctly, accurately or reliably. Without such documentation, it is impossible to know whether this software correctly executes the inherently complex functions and protocols needed to search a BitTorrent swarm for purported infringement.

In my experience, creating a software system without technical specifications or testing may be suitable to implement a web site for one's book club, but is not nearly good enough to build forensics software that could harm the health and safety of innocent bystanders when it fails to meet its intended purpose. According to the National Institute of Standards and Technology (NIST), test results must be repeatable and reproducible to be admissible as electronic evidence. Lacking technical proof of any kind that the software has been tested is compelling evidence that the IPP software does not meet NIST's standard. The Software Engineering Institute's Capability Maturity Model (CMM), meanwhile, confirms that IPP's software development process failed to meet NIST's repeatability standard, that the development must have been ad hoc at best, and that the code most likely contain hundreds of software bugs masking critical problems deep inside the code. In other words, the IPP software is unproven and should not be trusted for the forensics purposes as contemplated.

Under normal operating conditions, the IPP software downloads a miniscule amount (one or two pieces) of a video file from an IP address suspected of infringement. This means that the IPP software cannot distinguish infringing peers from those who have intentionally aborted downloads soon after having made a mistake. And it is unlikely that a user can view a partially download video file, especially if only a few pieces have actually been captured. This raises the question of whether detecting a few pieces is enough evidence to prove infringement.

I have also reported the conflict between the plaintiff's expert, Fieser, who implies that the IPP software captures all of the pieces of a movie from a defendant's IP address, reassembling it into a playable movie.

Relying only on the IP address is not enough to assert infringement in many cases. Shared use of a router by the subscriber, family, and friends in an area where neighbors could also camp onto the router represents a common situation where several users are sharing a router and the subscriber could be wrongfully accused of infringement. Router resets and infected computers overtaken by bots also represent scenarios where users could be wrongfully accused relying simply on a detected IP address.

Furthermore, I have also examined MaverickMonitor which has been the subject of attention of some of the same experts as those supporting the IPP software system. The infringement reports produced by these two forensics tools are virtually identical, as is their lack of technical documentation. I reviewed MaverickMonitor's code base which consists entirely of open source software amounting to 140,000 source lines of code (140 KSLOC). Given their reports are also virtually identical, and the same plaintiff experts have reported their opinions about both systems, I believe that the IPP software (NARS) and MaverickMonitor are composed of similar, if not virtually identical, software code bases.

Table of Contents

I refer to the IPP software also as "NARS" because the original expert reports I authored, and plaintiffs' have referred to this system as NARS (see [3a], [3b], [3c] and [3d] below.

The purpose of this document is to report my reliability assessment of NARS as it relates to Strike 3 Holdings Inc. vs John Doe, Case No. 2:17-cv-01731-TSZ and the motion by Strike 3 Holdings Inc. for Partial Summary Judgment filed 2/17/2019 in U.S. District Court, Western District of Washington for Seattle. I incorporate by reference my earlier expert report of March 15th, 2019 and all documents referenced therein.

My assessment is based on the evidence I have been provided to date. I have independently arrived at the opinions expressed in this report which depend on the accuracy of this evidence. My opinions are informed by my systems and software engineering qualifications, knowledge and experience.

Attached: **Exhibit A**, *Context of IPP Software* and **Exhibit B**, *Reliability Assessment of IPP Software*.

1. Software Engineering Standards and Guidance on which I Rely

I rely on the following standards and guidance in support of my expressed opinions:

a. **Exhibit C**, *BitStalker: Accurately and Efficiently Monitoring BitTorrent Traffic by* Buer et. al.: Describes their investigation and experiments evaluating the reliability of their proposed active monitoring method relative to traditional methods for identifying users sharing content across a BitTorrent network.

b. **Exhibit D**, *Validation of Forensic Tools and Software, A Quick Guide for the Digital Forensic Examiner* by Josh Brunty: Relies on the *Daubert Standard* and NIST's Computer Forensic Tool Testing Project (CFTT) providing guidance for validating software-based systems;

c. *Software Engineering Institute's (SEI) Capability Maturity Model (CMM):* Refined and widely applied for over two decades assisting organizations choose and tailor the most appropriate software behaviors, practices, and processes in order to achieve software reliably and sustainably goals.

d. **Exhibit E**, *Software Reliability Tutorial*, 2011-2015 by Gullo and Peterson: Pages 25 and 29 tabulate empirically derived software fault rates across the five (5) maturity levels of the CMM determined by leading software reliability experts in the field (Keene, Jones and Krasner).

e. *IEEE Software Engineering Standards including IEEE Std 12207, Systems and Software Engineering Software Life Cycle Processes*: Documents common frameworks with well-defined terminology for developing software-based systems from the requirements stage to system retirement.

2. My Relevant Qualifications

The opinions expressed in this report are drawn from my professional experience which is detailed in the **Annex** to this report, where I highlight my most relevant qualifications for conducting this reliability assessment, namely:

a. Independent validation and verification (IV&V) for External Affairs Canada

b. Quality, reliability, maintainability, safety, security, and software engineering for Hughes Aircraft

c. Software engineering practice leader for CGI Group and Hughes Aircraft

d. Software engineering courses for 10 universities including Oregon State, Portland State and TechBC.

3. Evidence Reviewed and Referenced

a. Skype Deposition of Michael Patzer, October 13, 2016.

b. Declaration of Michael Patzer, September 30, 2016.

c. Expert Report, Patrick Paige, October 26, 2016.

d. Supplemental Expert Report, Patrick Paige, December 16, 2016.

e. Supplemental Report and Opposition to Kal Toth and Bradley Wittman's Expert Report, Michael Patzer, Dec. 30, 2016.

f. Expert Report of Benjamin Perino, November 23, 2017.

g. Functional Description, IPP International IPTRACKER v1.2.1 appearing as Exhibit 1 of Declaration of Tobias Fieser in Support of Plaintiffs Motion for Leave to Take Discovery ... filed 08/16/11.

h. IPTRACKER software provided under Stipulated Protective Order Case No. 3:15-cvv-00907-AC.

i. Expert Witness of Dr. Simone Richter, April 2, 2014.

j. Expert Report of Robert D. Young, February 11, 2015.

k. Deposition of Robert D. Young, January 2, 2018.

l. Declaration of Stephen M. Bunting, Case 2:17-cv-00988-TSZ, Document 34, filed 2/05/2018.

m. Declaration of Tobias Fieser in Support of Plaintiff's Motion for Leave to Serve a Third Party Subpoena Prior to a Rule 26(f) Conference, US District Court, Western District of Washington at Seattle, 11/29/2017 [Docket 4-3].

n. Magistrate Judge Sheri Pym, Civil Minutes of US District Court Central District of California, Oct. 29, 2018

o. Declaration of Brandon Garcia-Paeth in Support of Defendant's Opposition to Plaintiff's Motion for Summary Judgment, Case no. 2:17-cv-01731-TSZ, 02/25/219.

p. Report of Bradley Witteman, re. Malibu Media vs. John Doe, 3:15-cv-04441-WHA, Jan. 20, 2017.

q. Declaration of Dr. Kal Toth in Support of Defendant's Opposition to Plaintiff's Motion for Summary Judgment, Case no. 2:17-cv-01731-TSZ, 02/25/219.

4. My Relevant Expert Reports

I have documented my reviews of some of the above documents in the following reports:

a. *Expert Report Re. Malibu LLC vs. John Doe*, Kal Toth, Dec 14th, 2016. I pointed out the lack of evidence supporting Patzer's claim in [3a] that NARS is free of defects (is flawless) using the well-known Therac-25 case to illustrate. I also addressed the inadequacy of testing by Paige [3c].

b. *Expert Report Re. Malibu LLC vs. John Doe, Rebuttal of Patzer Declaration and Paige Expert Report*, Dec. 28, 2017. I rebutted Patzer's declaration [3b] and Paige's supplemental expert report [3d] pointing out the absence of technical specifications, lack of software process, inadequate testing, etc.

c. *Expert Report Re. Malibu LLC vs. John Doe, response to Patzer Supplemental Expert Report*, Kal Toth, Jan 6th, 2017. I rebutted several claims by Patzer [3e] including that an agile process was used.

d. *Expert Report of Kal Toth Concerning Technical Report to Maverickeye*, May 10th, 2017. I compared the Maverickeye and Malibu technical reports demonstrating the equivalency of the systems generating them.

e. *Second Expert Report of Kal Toth Regarding the Maverickeye Case*, Dec 24, 2017. I critiqued the "Functional Description" provided in the Declaration of Fieser [3g], and provided a preliminary analysis of the IPTRACKER source code [3h] observing that NARS is adapted open source software.

f. *Third Expert Report: Assessment of MaverickMonitor Software Reliability,* February 27, 2018. I assessed the reliability of NARS, a software-based forensics tool used to detect the IP address of alleged copyright infringers of videos shared across BitTorrent networks.

5. My Assessment of the Reliability of the IPP Software

I have reviewed the IPP software (a.k.a. NARS) and the closely related MaverickMonitor system. The IPP software system and MaverickMonitor are operated in Germany. These closely related, if not identical, software-based tools detect IP addresses of users alleged to be infringing video copyrights by way of BitTorrent. Users install BitTorrent software ("clients") that support BitTorrent protocols to share files over the Internet including the distribution of software updates and videos. Patzer [3b], Perino [3f], and Richter [3i] have asserted that these tools are 100% accurate and free of defects. I do not agree with their assessments.

5.1 System Description (Context)

Exhibit A, *NARS System Context* depicts the context of my analysis *(follow* ❶, ❷, ❸, ❹ and ❺ on the figure).

5.1.1 BitTorrent Network ❶

Partially described in Exhibit D (BitStalker article), users cooperate with each other to share files using BitTorrent software modules ("clients") installed on their personal computers by leveraging BitTorrent Trackers and Torrent files that are hosted by various well-known service providers (e.g. PirateBay) across the web.

5.1.2 IPP Software System ❷

The IPP software operationalizes a system called NARS which is a tool used for forensics purposed to detect the sharing of selected video files of their customers among BitTorrent peers (users). The system is connected to the Internet by way of an ISP (Internet Service Provider). IPP operators specify the names of the video files to be tracked while the system repeatedly searches Bit Torrent "swarms" using an unspecified probing technique, and generates reports tracking the IP addresses of peers from which they have received "pieces" of the files, such pieces ranging from 16 Kbytes to 2 Mbytes. Shared video files detected by the system are typically 40 minutes in length and consume 200 to 600 Mbytes of storage on the average. The IPP software system reports users as infringing after receiving only a tiny fraction (1 or 2 pieces) of a given video file. All the pieces of a video file are rarely captured from a single IP address. Apparently, all pieces of a tracked file are usually captured from the collection of peer users participating a BitTorrent swarm.

5.1.3 No Evidence Supporting Claims that the IPP Software is Reliable ❸

In my expert reports [4a, 4b and 4c], I have documented the lack of technical documentation provided about the IPP software (NARS). I understand that the plaintiff did not disclose any of the technical documents requested during discovery. This means that there is no objective evidence that the IPP software developers produced any documents specifying the functions and protocols that the software is expected to execute repeatedly and correctly. The plaintiff and provided no objective evidence specifying the theory of system operation including the methods implemented by the software to probe the BitTorrent network to detect the origin (IP addresses) of copyrighted video files. No requirements or architectural design specifications showing how the software would correctly implement these methods and report findings were provided. Nor were the results of technical design and software reviews or system tests demonstrating that the deployed software works correctly and consistently under normal operating conditions and workloads provided. In addition, no objective evidence was provided of independent quality assurance, regression testing, bug tracking, configuration management, or release processes and procedures that would ensure that system performs it's intended functions on a continuing basis throughput its operational life. In the absence of technical documentation it is impossible to know whether the IPP software correctly executes even the most rudimentary functions and features expected of a simple web site. Given that the IPP software could harm the health and safety of innocent bystanders by enabling wrongful accusation, I find it alarming to know that such unproven software is being used for such forensics purposes.

5.1.4 Unreliable Reporting of IP Addresses ❹

Given the virtual absence of technical artifacts provided to me, I can only conclude that the IPP software cannot be relied upon and must therefore be unreliable as additionally argued below. This may partially explain why IPP has not offered the software as a commercial product. As discussed further below, this implies that the software likely contains many latent (hidden) defects that could cause the software to incorrectly match IP addresses to captured pieces of tracked and captured videos. Such deep-rooted defects in the code can cause silent and subtle errors, particularly in heavily loaded concurrent processing systems. Consider the Therac-25 case I documented in Toth [4a] where three patients were killed and another three were severely injured due to massive radiation caused by latent software defects.

Experts connected with the present case and the related cases have provided no visibility into the technical implementation of the IPP system. The plaintiffs' investigations have depended on rudimentary test cases conducted by Paige [3b], Richter [3i], Bunting [3l] and other of their experts. It is evident to me that their experts ran simple demonstration tests aimed at convincing non-technical observers simply that the IPP software "works". Given the lack of technical documentation, these tests do not convince me that the IPP software works correctly most of the time or even part of the time. To date I have not received any evidence that the software was subjected to tests designed to show it operates reliably and correctly under representative workloads, busy periods or failure modes.

As documented in my expert reports [4d, 4e and 4f], I have examined MaverickMonitor which is also advertised as a BitTorrent infringement detection system. The reports produced by these two forensics tools are virtually identical. The IPP software and MaverickMonitor are also identical in the lack of technical documentation provided.

In my expert report [4e], I had the opportunity to review MaverickMonitor's code base which consists entirely of open source software amounting to 140,000 source lines of code (140 KSLOC). Given their reports are virtually identical, and the same experts for plaintiffs have reported their opinions about the both systems, I am of the opinion that the IPP software (NARS) and MaverickMonitor are composed of similar, and perhaps identical, software code bases.

If provided technical documentation, objective evidence of the software engineering development and maintenance processes conducted to develop the IPP software, including reviews, tests cases, procedures, and test results, and the IPP software's source code, I would be pleased to reexamine my reliability assessment and conclusions.

5.1.5 Conflicting Representations and Data Concerning Reported Infringement ❺

I have duly observed a conflict between representations made by the plaintiff's expert Fieser, and data produced by the IPP software that was provided by the plaintiff:

(a) First of all, the plaintiff's expert, Fieser, in [3m] (page 3, item 9) declares "IPP's software additionally analyzed each BitTorrent 'piece' distributed by Defendant's IP Address. It verified that reassembling the pieces using a specialized Bitorrent client results in a fully capable movie."

(b) Judge Pym [3n] in the minutes of Oct. 29, 2018 (footnote on page 5) appears to interpret Fieser's declaration to mean that all pieces of the copyrighted work were transmitted by the defendants.

(c) However, analysis of PCAP data provided by the plaintiffs to the defendants provide contrary evidence:

   i. Garcia-Paeth [3o] describes his analysis of the *PCAP data* files - one *PCAP* for each of the 87 movies tracked by the IPP software and attributed to the defendant. These movies ranged from 200 MB to 600 MB totaling 26.6 GB in all. He explains that at 16KB per PCAP, over 1.6 million PCAPS would have had to be received from the defendant to capture all of content of these 87 movies. However, only 405 PCAPs were actually received from the plaintiff. He also calculated that between 0% to 0.016% of each movie was actually captured from the tracked IP address.

   ii. Witteman [3p] similarly analyzed 23 PCAP data for 23 movies that demonstrated that the Excipio system (a.k.a. NARS and IPP) actually captured only one (1) piece of each movie.

Mr. Fieser's declaration [3m] conflicts with the PCAP *data* which provides objective evidence that the IPP software captures only a miniscule amount (about 0.007%) of a movie from a monitored IP address.

5.1.6 Abandoned Sharing Reported as Infringement ❻

Previously, I have also commented about the problem of abandoned BitTorrent sharing. An innocent BitTorrent user who normally uses BitTorrent to share content legally, could accidentally click on a link and start unintentionally capturing a copyrighted video file. She may not notice this problem until returning with her mug of coffee. She then realizes her BitTorrent client software is capturing unwanted content, cancels her download, and deletes the partially downloaded video file. If the IPP software happened to be tracking the sharing of this copyrighted content at the time of her accidental click, IPP could well detect one or two pieces and report her as infringing copyright.

5.1.7 Identity of Purported Infringer Ambiguous ❼

The IPP software normally identifies purported infringers by searching BitTorrent Trackers using the names of copyrighted video files they wish to track. Typically, IPP tracks many IP addresses simultaneously. Exhibit A illustrates a representative household with a single Internet router connected to an ISP (e.g. Comcast). The router may be available for use by the subscriber, family members, tenants, and guests. Neighbors and (drive-by/walk-by) "lurkers" may also be able to connect to the router either because the router is password-less, or because the owner never bothered to change the default password and the lurker knows the common routers and defaults used when they come out of the box. It may also happen that the computer of a member of such a household becomes infected by way of an email phishing exploit which enabled remote malicious party to download copyrighted video content in BitTorrent thereby implicating the owner of copyright infringement.

5.1.8 Plaintiff's Investigation Relies on Ambiguous, Incorrect, Incomplete and Unproven Factors ❽

Exhibit A also depicts the investigation process conducted on behalf of the plaintiffs. I believe this process relies excessively on the asserted accuracy of the IPP software. The IPP software's lack of specifications and processes suggests that it is an unreliable software-based tool that could accuse innocent parties of infringement. This means that under heavy workload conditions the software could inconsistently and inaccurately map monitored pieces of video content to detected IP addresses. Meanwhile, the IPP software only captures a small number of pieces from the purported infringer's IP address. And it could happen that an innocent party downloads the wrong file, aborts the session, and deletes the file, but is reported as infringing. Finally, the IP address happens to have about 10 users sharing the computer – the subscriber could be wrongfully accused.

In other words, the copyright investigation process relies on a combination of ambiguous, incorrect, and incomplete information while using unproven software without objective evidence of reliability.

5.2 IPP Software Reliability Assessment

My reliability assessment explores the following questions:

- Is the IPP software reliable enough to conduct forensics investigations?
- Is partial evidence of downloaded videos sufficient evidence to conclude copyright infringement?
- Is a monitored IP address enough to suspect an ISP subscriber, family and friends of infringement?

Please refer to Exhibit B which depicts my reliability assessment in the context laid out in Exhibit A. My assessment examines the likelihood that infringement is correctly detected. The figure in Exhibit B depicts four branches of my reliability analysis: ❶, ❷, ❸, and ❹.

5.2.1 Demonstration Tests ❶

The demonstration tests described by Paige, Richter and Bunting involved setting up three or four test computers with installed BitTorrent clients connected to Internet service providers configured to share a few predetermined video files using BitTorrent. All of these test setups confirmed that all the pieces (100%) were detected by the IPP software.

Since first examining how the IPP software works, I wondered why the system generates an infringement report after only few pieces of a video have been captured from a monitored IP address when in "forensics mode", while all pieces are captured in "demo mode". After some reflection, I began to realize why these test cases demonstrated that all of the pieces of the test video files could be detected from a test computer. Simply stated, these tests demonstrate nothing about the reliability of the IPP software when operated under real-world operating conditions. For example, they do not attempt to address the problems associated with routers using dynamic IP addressing (i.e. IP address resets), or conduct tests that try to determine if more than one user is attached to the router, or that the user has aborted an unintended download, or that a user has shut down because all the pieces had been received from other peers in the swarm. At the very least, these tests should have simulated router resets by powering them down and rebooting them during file sharing, and by running scenarios where BitTorrent users abort the downloading of shared video files before completion. Such operationally representative tests would have confirmed whether the IPP software could cope with unusual circumstances and events, and whether all the pieces of a file could be received peers operating normally in the swarm rather than test computers set up under synthetic operating conditions.

Another shortcoming was that these demonstration tests did not document the operating workloads during the test runs, or the number peers.participating in the BitTorrent swarm during the period of the tests.

5.2.2 Number of Detected Pieces of Copyrighted Content ❷

a. As already mentioned, the IPP software (NARS) reports detected videos as infringing after only a few pieces are downloaded from a monitored IP address. It appears that the IPP software does not attempt to detect all pieces of a shared video file from a monitored IP address before reporting infringement.

b. I also mentioned, that the fact that the IPP software assumes infringement after only 1 or 2 pieces have been detected from a monitored IP address means that someone aborting a session because they made an honest mistake, would be wrongfully accused of copyright infringement.

c. I understand that partially downloaded Bit Torrent files may require technical skills to view them by means of standard video players. My search of online blogs confirm that VLC and AVI Preview are two such video players that can be used to view video files that have been partially downloaded using BitTorrent client software. However, the experience is "choppy" in proportion to the number of missing pieces and how contiguous they are. Furthermore, these players will not render a partially downloaded video if the first part of the video is missing. Since BitTorrent shares pieces randomly, a user is unlikely to be able to play the content until a large percentage of a given video is captured. This means that users attempting to do this need to have technical knowledge and skills, as well as patience, to view such partially downloaded videos. Whether being in possession of such partially downloaded and potentially unplayable videos constitutes infringement is a legal question outside my purview.

5.2.3 IPP Software Reliability ❸

a. **Unproven Software-based Forensics Tool:** Brunty's article ([1b] Exhibit D) explains that NIST standards require that forensics software and tools be repeatable and reproducible. Given that virtually no technical specifications or processes have been provided to support the claim that the IPP software (NARS) was developed using best software engineering practices, one can only conclude that the IPP software fails to meet the NIST standard. Using Brunty's arguments, it can be argued that NARS is not reliable enough to detect IP addresses consistently and correctly, and hence IPP infringement reports not be reliable enough to be admissible as electronic evidence for such forensics purposes.

b. **Large Number of Latent Software Faults:** I have studied, conducted software process assessments, and taught the widely respected principles of the Software Engineering Institute's Capability Maturity Model (CMM) [1c] throughout my career. I rely on the *software reliability tutorial by* Gullo and Peterson ([1d] Exhibit E) which tabulates empirically derived software fault densities for each CMM level from CMM Level 1 to CMM Level 5. Given the dearth of specifications and processes used to develop the IPP software, I conclude that the IPP software must have been developed at the lowest level, namely, CMM Level 1 "Initial" (known informally as the "ad hoc" level). Using Gullo and Peterson's CMM fault density table for CMM Level 1, and my estimate for the software size derived from [3e] of 140,000 software lines of code (140 KSLOC), I estimate that the IPP software has between 700 and 4,200 latent faults (a.k.a. defects). Of course, only a portion of these defects (say 10%) would have critical impacts on operations. However, such high fault density levels associated with CMM Level 1 do lend credibility to NISTs standard for forensics tools, namely, that software development incorporate processes that render software systems delivering repeatable and reproducible results. In other words, NIST's standard for forensics software tools aligns with CMM Level 2 "Repeatable" and would yield a 10 fold decrease in latent faults in the resulting code. The lack of technical specifications and best software engineering is precisely why I assert with confidence that the IPP software is unproven and unreliable.

c. **False Positive Rate is about 11%:** The BitStalker article ([1a] Exhibit C) by Bauer et.al. states that traditional ping probing techniques used to identity file sharing in BitTorrent networks detect IP addresses falsely about 11% of the time. The article demonstrates that BitStalker's proposed active probing technique can achieve accuracy close to 2%. However, validating information, such as a theory of operation document, has not been provided to confirm which probing method is used by the IPP software. This means that with the information that has been provided by the plaintiff, the best the IPP software can hope to achieve would be an 11% false positive rate. Of course this rate could only be achieved if the IPP software was shown to be truly free of critical defects which CMM Level 1 strongly suggests is not the case.

5.2.4 Accuracy with which an IP Address can Identify Infringer ❹

It has been asserted that the IP address reported by the IPP software is a strong enough indicator of infringement to warrant the issuance of a subpoena to the ISP. However, there are several scenarios where an innocent party, especially the subscriber, could be wrongfully accused. Exhibit A depicts some of these cases.

a. It appears that the IPP software is unable to prove that all the traffic detected from a given IP address passed through the same physical router over a significant period of time. Neither does the IPP software detect if a router using an IP address is password-protected. Furthermore, IPP cannot be sure whether there is only a single person using a given router, or a large number of persons are routinely using the router to access the Internet.

b. For example, households may include the subscriber, several family members and/or tenants, visiting guests, as well as neighbors and lurkers within range of their Internet routers. Although cautious subscribers password-protect their routers, default passwords are often left unchanged and therefore guessable, and some people prefer leaving their passwords open. Sometimes passwords are cracked by walkers-by or a drive-by (default router passwords are infrequently changed and guessable).

c. Exhibit A depicts 10 potential users. Any one of them could be an infringing user detected by the IPP software. This scenario illustrates that the other 9 persons are innocent bystanders. This means that there is a 90% change that someone could be wrongfully accused.

d. Although the population within and surrounding a household varies, in the absence of knowing where the IP address is located at any given time means that it is unreasonable to assume that a detected IP address is attributable to a single person (i.e. the subscriber).

e. The IP addresses allocated to routers are sometimes reset by ISPs; users may reset them whenever the router hangs; and some user may routinely reset them to guard against cybersecurity attacks. Power outages will also reset routers when power returns. Assume that the average router is reset, say, four times a month. Now let's assume that an infringer using our ISP is being actively monitored by the IPP software system on a given IP address. That same day the infringer's IP address is reset and allocated to your router. This means that there is a risk that the IPP software will assume you are the infringer, enabling a plaintiff to send a subpoena accusing you of infringement.

f. Another possibility is by way of a phishing attack. Your computer is infected and a botnet takes control of your computer in the background, using it as a proxy to execute various unauthorized activities, including illegal video file sharing by way of BitTorrent. The IPP software could identify the IP address of your router and hence accuse you, the ISP subscriber, of copyright infringement.

5.2.5 BitTorrent Client Software Accuracy and Reliability

The IPP software system (NARS) relies on the correct operation of BitTorrent client software used by peer users operating across the BitTorrent network when they collaborate with each other across a given swarm to share content. In addition to the IPP software system itself, these software clients must implement the BitTorrent protocols, including packet formats, accurately and consistently to provide assurances that the system, as a whole, reliably and correctly requests and captures all the pieces comprising a given media file (movie) subsequently attributed to a purported infringer by the IPP software.

No mention has been made in any of the depositions, declarations or expert reports that I have received and reviewed (i.e. those referenced herein) about the reliability of any of the various open source and proprietary software clients available and used to share media across a swarm. This leaves an additional critical gap in the plaintiff's methodology supporting assertions that NARS accurately and consistently reports alleged infringers.

6. Summary of Observations and Findings

Plaintiffs' experts have asserted that the IPP software (NARS) is 100% accurate and free of defects [4a]. In my experience, claiming that operational software is defect-free is not credible. Neither is asserting that a complex software-based system detects infringement flawlessly.

If a software-intensive system is expected to be highly accurate, and advertised as such, the software engineering and development processes must be sufficiently capable and mature, should be guided by credible standards, and be supported by experienced personnel and proven tools. There is no evidence that capable software processes, technical specifications, comprehensive testing, or quality assurances were conducted in the development of the IPP software. My reviews of Patzer [3b], Perino [3f], Fieser [3g], and Richter [3i] confirm that such objective evidence including theory of operation, architectural design, testing, and other software engineering processes used to develop the software was not provided.

Principle Findings of my Reliability Assessment: The lack of technical specifications and process documentation confirm that the IPP software system (NARS) does not meet NIST's standard of repeatability and reproducibility for forensics software tools. I can only conclude that the IPP Software must have been developed using an ad hoc software engineering process consistent with CMM Level 1. This in turn implies that the IPP software is unproven, with a significant number of latent software faults (bugs) that could be yielding inaccurate results. Therefore, this software should not be trusted for the forensics purpose of detecting copyright infringement of movies by way of BitTorrent file sharing. Clearly, the IPP software is not a reliable solution capable of delivering repeatable or reproducible results needed to field an operational forensics software tool that could harm the safety and health of innocent bystanders.

It appears that the IPP software cannot distinguish infringing peers from those who have aborted a download having realized they made a mistake. This problem could be solved if the IPP software was programmed to download all of the pieces of a file before reporting infringement. However, it could be that the IPP software has been programmed to only download a few pieces before reporting infringement. The other possibility is that under normal operating conditions, the IPP software is incapable of downloading all the pieces of a video file from an IP address suspected of infringement. Recognizing this limitation, IPP may have redirected its strategy to implicate as many infringers as possible by downloading only a few pieces before reporting infringement.

Meanwhile, it is unlikely that ordinary users will be able to view partially downloaded video content, especially given that the IPP software only captures a miniscule amount of a movie from a monitored IP address. This raises two questions:

a. Is detecting partial capture of a copyrighted movie enough evidence to report infringement?

b. Should a forensics tool like IPP be expected to download all pieces of a movie before reporting infringement?

Finally, relying only on the IP address to assert infringement is not enough in many cases. Shared use of a router by the subscriber, family, and friends in an area where neighbors could also camp onto the router represents a common situation where a number of users sharing a router could be wrongfully accused of infringement. Router resets and infected computers overtaken by bots also represent scenarios where users of a given router could be wrongfully accused.

Possibly Undisclosed Problem: Given the random nature of BitTorrent's sharing protocol, it may not be possible in many circumstances for the IPP software to capture all pieces of a targeted file from a monitored IP address. This may well be because BitTorrent is designed for peer users to share pieces with many other peers. Once a peer has collected all the pieces wanted, he/she would most likely close the BitTorrent client and stop responding to IPP software requests for pieces. This means that the IPP software is highly unlikely to be able to capture all pieces of a tracked video from any given IP address in a BitTorrent swarm.

These facts may explain why the IPP software is able to detect all the pieces of test videos configured by Paige, Richter and Bunting. Because their test files have uninteresting titles, are watermarked, and are relatively short, other BitTorrent peers will not be interested in sharing pieces with the test computers. Meanwhile, the test computers can be programmed to wait until all the pieces have been shared before shutting down.

Fieser's Declaration: Fieser declares, [3m] page 3, item 9, that "IPP's software additionally analyzed each BitTorrent "piece" distributed by Defendant's IP Address. It verified that reassembling the pieces using a specialized Bitorrent client results in a fully capable movie." In 5.1.5 I explain that Fieser's assertion misrepresents the facts of the matter. He apparently asserts that the IPP software captures all of the pieces of a movie from a defendant's IP address, reassembling it into a playable movie. Objective evidence demonstrates that IPP's software captures only a tiny portion of a movie from a monitored IP address, which by all accounts, is an ambiguous indicator of a user's true identity. Taken together, these facts provide compelling evidence that Fieser's declaration is not true.

My rate is $350.00 per hour.

K.C. Toth

Signed under the Penalty of Perjury,
Kal Toth (Kalman C. Toth), Ph.D., P.Eng.

Annex: My Most Relevant Experience and CV (Kal Toth)

Kalman C. Toth, Ph.D., P. Eng.

304-1132 SW 19th Ave Portland OR 97205
kalmanctoth@gmail.com 503.984.3531

Security, Software, Quality, and Systems Engineering Professional

Background / Experience:

- In leadership positions with technology companies in the fields of security, software and IT
- Software, systems and security-related engineering innovator, consultant, and change agent
- Technology solutions and consulting in government, financial and selected industry sectors
- Cybersecurity, identity management, e-commerce, mobile computing, distributed systems, networking, communications, and databases.
- Air traffic control; real-time stock quotation for mobile devices; search and rescue system, security devices and gateways; global secure messaging network; on-line learning systems
- Systems engineering evangelist: traditional and agile software development, project management
- Software engineering, IT and project management courses and training for working professionals.

Competencies:

Systems, security, software and quality engineering, Strategic and business planning, Project management, Digital Identity technology and security engineering, e-learning/distance education

Citizenship and Residency: U.S. Citizen, U.S. Resident, also a Canadian Citizen

Languages: English (mother tongue), Hungarian (father tongue), and French fluency

World: Early IT career with World Health Organization, Geneva, Switz; well-travelled in Europe

Education:

Ph.D. Electrical and Computer Systems Engineering
M. Eng. Systems Engineering and Computer Science
B. Eng. Electrical Engineering

Professional Engineer (P. Eng.): BC Association of Professional Engineers and Geoscientists
Training/Education Courses: E-commerce, SW engineering, project management, prof. issues (i.e. IP)
Pacific Northwest Software Quality Conference: Board member and 2013 Conference Chair
Portland State University: Faculty Senate Budget Committee; Intellectual Property/DistEd Taskforce
Goose Hollow, Portland Oregon: neighbourhood association Board of Directors

Patents (issued and pending):

"*Electronic Identity and Credentialing System*", US Pat. 9646150, 20/17.

"*Methods for Using Digital Seals for Non-Repudiation of Attestations*", US Pat. 9900309, Feb. 20, 2018.

"*Registering and Acquiring E-credentials using Proof-of-Existence and Digital Seals*, US Pat. 10127378, Nov. 13, 2018.

"*Architecture and Methods for Self-Sovereign Digital Identity*", Pending, filed Nov. 12, 2018.

"*Portable Caching System*", submitted in 2007, abandoned in 2015.

Intellectual Property Cases: Expert Reports

- *Eloqui v. Nuance,* for plaintiff, patent infringement, 2 expert reports, 2018.
- Malibu v. John Doe, for defendant, copyright infringement, 3 expert reports, 2016-17.
- *Dallas Buyers Club v. Huzsar*, for defendant, copyright infringement, 2 expert reports 2017-18.
- *Clear Skies Nevada v. Anderson et. al.*, for defendant, copyright infringement, 1 expert report 2018.
- *Strike 3 Holdings v. John Doe*, for defendant, 2018, 2 reliability assessment reports, 2019.
- *Clear Skies Nevada v. Kainu*, for defendant, 2018, designated expert.

Key Positions / Appointments / Expert Reports / Publications / Courses listed below

See also http://www.linkedin.com/pub/kal-toth/2/60b/b19

Key Positions / Appointments

NexGenID (2013 - present), CEO and CTO

- Created innovative identity and credentialing technology: "Electronic Identity and Credentialing Technology" per above-referenced patent and patent-pending identity technology
- Developed detailed functional specification and proof-of-concept for digital identity prototype_(Android-based)

aTrust Inc. (2012 - 2013), Chief Technology Officer (CTO)

- Progressed startup's vision for digital identity, technology roadmap, and product-line development strategy
- Built and maintained partner/vendor relationships in technology and banking sectors
- Managed and evaluated the distributed development team's progress and performance

Portland State University (2003-12), Executive Director and Associate Professor

- Directed, enhanced and evolved the Oregon Master of Software Engineering (OMSE) into a fully online learning program for working software professionals in Oregon's hi-tech sector
- Delivered software engineering, project management, quality engineering, distributed team, estimating, and architectural design courses and seminars – both face-to-face and online
- Investigated identity management technologies targeted at the healthcare and banking sectors creating the "Persona Concept", a framework for managing electronic credentials and private data of users across PCs, smart cards, smart phones, and other personal devices

Oregon State University (2001-2003), Associate Professor Computer Science

Technical University of British Columbia (1999-2001), Assoc. Professor Information Technology

Datalink Systems Corp. (1997-99), Vice President Engineering

- Following a light-weight agile software development process, directed development and operations
- Led the development of a web-based service and payment processor for delivering real-time stock quotes, news, sports, and other services to wireless devices - pagers and cell phones
- Worked with marketing/support to develop requirements and rapid response to user problems
- Removed security weaknesses of the previously deployed service center
- Developed replacement architecture with scalability, backup and recovery features

Hughes Aircraft Systems Division (1992-95), Director of Quality

- Led quality, reliability, maintainability, availability and system safety teams for five (5) large air traffic control projects (Canada, Canadian military, Switzerland, Indonesia and China)
- Leading member of the core team transitioning division from a waterfall to an iterative software process which guided the development of Canada's $400M air traffic control system ("CAATS")
- Created a new process infrastructure for the division's policies, practices and procedures

CGI Group Inc. (1988-1992), Vice President Systems Engineering, Vice President Total Quality

- Practice leader across CGI's 10 regional offices for project management, software engineering, quality engineering, configuration management, and software estimating
- Led process improvement initiatives across CGI's US and Canadian offices
- Developed and initiated a strategic plan to implement a company-wide total quality process
- Conducted independent verification and validation of a $50M project to develop a globally secure network across Canada's embassies abroad for External Affairs Canada
- Developed an innovative information security analysis model for Defence Canada

Intellitech Canada Ltd. (1983-88), Founder and President

- Founded Intellitech, growing it into a 25-person systems engineering and consulting firm
- Conducted numerous design and development projects for distributed information systems, networks and security gateways for military, government and industry clients
- Led the development of Intellitech's secure packet-network product and the delivery of prototypes to Communications Canada – funded by the Canadian National Research Council and the Bank of Montreal, and sponsored by the Communications Security Establishment

Carleton University (1980-83), Assistant Professor, Systems Engineering and Computer Science

Expert Reports: Intellectual Property Cases

- *Eloqui v. Nuance,* for plaintiff, patent infringement, 2 expert reports, 2018.
- *Malibu Media, LLC v. John Doe*, for the defendant, 2016-17, three expert reports assessing and rebutting other expert reports concerning the reliability of a software system detecting copyright infringement.
- *Dallas Buyers Club, LLC v. Huzsar*, for the defendant, 2017-18, three expert reports assessing and rebutting other expert reports concerning the reliability of the software systems detect copyright infringement.
- *Clear Skies Nevada, LLC v. Anderson*, Richards and Hancock, for the defendant, expert report assessing the reliability of concerning the reliability of a software system detecting copyright infringement.
- *Strike 3 Holdings, LLC v. John Doe*, for the defendant, 2018, two reliability assessment reports, 2019.
- *Clear Skies Nevada, LLC v. Kainu*, for the defendant, 2018, designated expert.

Publications and Seminars in the Field of Security, Identity and Authentication

- Kalman C Tóth, Brewing Next Generation Identity, Pacific Northwest Software Quality Conference, Oct 2015
- Kalman C. Toth, A Practical Identity Management Reference Implementation, International Conference on Computers and Their Application (CATA), Honolulu, Hawaii, March 28-30, 2007
- Kalman Toth, Persona Concept for Web-Based Identity Management, 2006 International Conference on Privacy, Security and Trust, UOIT, Newmarket, Ontario, Oct 30-November 1 2006
- "Identity Management Systems", tutorial for IEEE International Computer Software and Applications Conference (COMPSAC), Chicago, September 2006
- Information security seminars for the Assoc. of Prof. Engineers and Geoscientists of B.C., 2002 and 2006
- K.C. Toth, M.Subramanium, Requirements for the Persona Concept, Requirements for High Assurance Systems (RHAS'03) workshop, Monterey, CA, September 9, 2003
- K.C. Toth, M. Subramanium, The Persona Concept: A Consumer-Centered Identity Model, MobEA (Emerging Applications for Wireless and Mobile Access), Budapest, Hungary, May 2003
- K.C. Toth, M. Subramanium, Persona Concept for Privacy and Authentication, International Business & Economics Research Journal, June 2003
- K.C. Toth, M. Subramanium, I. Chen, Persona Concept for Privacy and Authentication, International Applied Business Research Conference, Acapulco, Mexico, March 2003; recipient of best paper award
- K.C. Toth, M.Donat and J. Joyce, Generating Test Cases from Formal Specifications, 1996 International Council of Systems Engineering (INCOSE) Symposium, July 1996
- M.W.L. Dennison, K.C. Toth & J.F. Clayton, Using a Practical Approach to Threat/Risk Analysis, Third Annual Canadian Computer Security Conference, Ottawa, May 14-16, 1991
- K. Toth, Information Security Architectures, AFCEA '90 (Armed Forces Communications & Electronics Association Technical Conference), Hawaii, November, 1990
- K.C. Toth, Security Architectures for Information Networks, AFCEA Canada '90, April 1990
- H. Adra, J. Allen, K. Toth, Trusted Integrated Project Support Environments, Second Annual Canadian Computer Security Conference, Ottawa, March 1990
- K. Toth, Towards an Improved Information Security Model, 1st Canadian Comp. Security Conf, January 1989
- K. Toth, Security Management in Data Networks, 1st Annual Canadian Computer Security Conf, Jan 1989
- AC Capel, C Laferriere & K.C Toth, Protecting the Security of X.25 Comm's, Data Com Mag, November 1988

- M.W.L. Dennison, K.C. Toth & J.F. Clayton, Using a Practical Approach to Threat/Risk Analysis, Third Annual Canadian Computer Security Conference, Ottawa, May 14-16, 1991
- K. Toth, Information Security Architectures, AFCEA '90 (Armed Forces Communications & Electronics Association Technical Conference), Hawaii, November, 1990
- K.C. Tóth, Security Architectures for Information Networks, AFCEA Canada '90, April 1990
- K. Toth, Towards an Improved Information Security Model, 1st Canadian Comp. Security Conf, January 1989
- K. Toth, Security Management in Data Networks, 1st Annual Canadian Computer Security Conf, Jan 1989
- AC Capel, C Laferriere & K.C Toth, Protecting the Security of X.25 Comm's, Data Com Mag, November 1988

- System Security and Recovery Procedures, Datalink Systems Corp, January 1999
- "EDI and Security", CGI Group report, Dec. 1990
- "COSICS Security Verification Plan", Intellitech report to External Affairs, December, 1988
- "Information Security Model", report to National Defence, November 15, 1988
- "Data Encryption Equipment Specification", Internal report specifying the components of CryptoNet,

Intellitech's X.25/DES product, 1986

- "A New Implementation Strategy for Secure Operating Systems", Intellitech Report, March 1986
- "Design and Security Considerations for a Gateway to Interconnect SAMSON and DATAPAC", Report to the Department of National Defence, 1980

Conferences and Journal Publications

- Kalman C Toth, Brewing Next Generation Identity, Pacific Northwest Software Quality Conference, Oct'15
- Kalman C Toth, Herm Migliore, Critical Factors Characterizing Projects & Lifecycle Models, PNSQC, Oct'13
- Kalman Toth, Learning Software Engineering Online, Pacific Northwest Software Quality Conference, Oct'11
- Kal Toth, Organizational Approach for Sustaining E-Learning in Large Urban University, Future of Ed, Jun'11
- Kal Toth, Software Engineering Online and Hybrid Learning Models at PSU, CATA, March, 2011
- Kal Toth, Raleigh Ledet, Lessons Learned about Distributed Software Team Collaboration, PNSQC, Oct'10
- Kal Toth, Software Estimating: Navigating to Landing Zone, Computers & their App's, Honolulu, HI, Mar'10
- Kal Toth et. al., Distributed Software Engineering Team Collaboration, poster session, PNSQC, October 2009
- Kal Toth, Software Estimating, Flexibility and Principled Negotiation, Computers and their Applications in Industry and Engineering (CAINE), San Francisco, November, 2009
- Kal Toth, Selecting Software Estimating Techniques that Fit the Software Process, Pacific Northwest Software Quality Conference (PNSQC), Portland, Oregon, October, 2008
- Dan Brook, Kal Toth, Levels of Process Ceremony for Software Configuration Management, Pacific Northwest Software Quality Conference (PNSQC), Portland, Oregon, October, 2007
- Kalman C. Toth, A Practical Identity Management Reference Implementation, International Conference on Computers and Their Application (CATA), Honolulu, Hawaii, March 28-30, 2007
- Kal Toth, Experiences with Open Source Software Engineering Tools, IEEE Software, Nov/Dec 2006
- Kalman Toth, Persona Concept for Web-Based Identity Management, 2006 International Conference on Privacy, Security and Trust, UOIT, Newmarket, Ontario, Oct 30-November 1 2006
- L. Grove, R. Hickman, W. Matthews, K. Toth, Open Source Software Engineering Tools, Pacific Northwest Software Quality Conference (PNSQC), Portland, Oregon, October 12-13, 2004
- K.C. Toth, M.Subramanium, Requirements for the Persona Concept, Requirements for High Assurance Systems (RHAS'03) workshop, Monterey, CA, September 9, 2003
- K.C. Toth, M. Subramanium, The Persona Concept: A Consumer-Centered Identity Model, MobEA (Emerging Applications for Wireless and Mobile Access), Budapest, Hungary, May 2003
- K.C. Toth, M. Subramanium, Persona Concept for Privacy and Authentication, International Business & Economics Research Journal, June 2003
- K.C. Toth, M. Subramanium, I. Chen, Persona Concept for Privacy and Authentication, International Applied Business Research Conference, Acapulco, Mexico, March 2003; recipient of best paper award
- K.C. Toth and S. Nagboth, A Constraint-Based Personalization Model for E-Business Applications, International Applied Business Research Conference, Acapulco, Mexico, March 2003
- K.C. Toth, S. Nagboth, Intelligent Agents for Business Applications Using Constraint-Based Personalization, International Business & Economics Research (IBER) Journal, May 2002
- K.C. Toth, Software Product Evolution in the Classroom, American Society for Engineering Education / PSW, Fresno, California, April 8, 2002
- K.C. Toth, Simulating (Software) Product Evolution in the Classroom, The Western Canadian Conference on Computing Education (WCCCE), Nelson, British Columbia, May 3, 2001
- K.C. Toth and H. Todino, Instant Internet Intelligence for Wireless Business Applications, International Applied Business Research Conference, Cancun, Mexico, March 2001
- D Cyr, H Trevor-Smith, T Schiphorst & K.C Toth, A Web-Enabled Case Study in Project Management, International Business Education and Technology Conference, Cancun Mexico, March 2001
- K.C. Toth, M.Donat and J. Joyce, Generating Test Cases from Formal Specifications, 1996 International Council of Systems Engineering (INCOSE) Symposium, July 1996
- R. John, J. Madhur, R. Stewart, K. Toth, Software Quality Metrics Process For Large Scale Systems Development, 1996 INCOSE Symposium, July 1996
- K.C. Toth, J.J. Joyce, J. Masters, G. Pelletier, Precise, Unambiguous, Machine-Readable ATC Standards: Use of "Formal Methods" in the ATC Industry, ATCA Conference Proceedings, September 1995

- K Toth & J. Joyce, Industrialization of Formal Methods Through Process Definition, feature paper at the 1995 National Council on Systems Engineering Symposium, July 1995
- T. Paine, P. Kruchten & K. Toth, Modernizing ATC Through Modern Software Methods, Proceedings of the 38th Annual Air Traffic Control Association, Nashville, Tennessee, October 1993
- M.W.L. Dennison, K.C. Toth & J.F. Clayton, Using a Practical Approach to Threat/Risk Analysis, Third Annual Canadian Computer Security Conference, Ottawa, May 14-16, 1991
- K. Toth, Information Security Architectures, AFCEA '90 (Armed Forces Communications & Electronics Association Technical Conference), Hawaii, November, 1990
- K.C. Toth, Security Architectures for Information Networks, AFCEA Canada '90, April 1990
- H. Adra, J. Allen, K. Toth, Trusted Integrated Project Support Environments, Second Annual Canadian Computer Security Conference, Ottawa, March 1990
- K. Toth, Towards an Improved Information Security Model, 1st Canadian Comp. Security Conf, Jan 1989
- K. Toth, Security Management in Data Networks, 1st Annual Canadian Computer Security Conf, Jan 1989
- AC Capel, C Laferriere & K.C Toth, Protecting the Security of X.25 Comm's, Data Com Mag, November 1988
- K.C. Toth, S.A. Mahmoud, J.S. Riordon, Query Processing Strategies in a Distributed Database Architecture, Distributed Data Systems, North-Holland Publishing Co., 1982
- K.C. Toth, S.A. Mahmoud & J.S. Riordon, An Approach to Query Processing in Distributed Databases, Proceedings of the Sixth International Conference on Very Large Data Bases, Montreal, 1980
- Kalman C. Toth, Distributed Database Architecture & Query Processing Strategies, Ph.D. Carleton U 1980
- S.A. Mahmoud, J.S. Riordon & K.C. Toth, Distributed Database Partitioning & Query Processing, G. Bracchi and G.M. Nijessen (ed), Data Base Architecture, IFIP, North Holland, 1979
- S.A. Mahmoud, J.S. Riordon and K.C. Toth, Distributed Database Partitioning and Query Processing Strategies, IFIP Conference on Database Architecture, Venice, June, 1979
- J.S. Riordon, S.A. Mahmoud, K.C. Toth & O. Sherif, Distributed Database Architecture and Query Processing, CIPS/DPMA, Quebec City, June 1979
- K.C. Toth, S.A. Mahmoud, J.S. Riordon, O. Sherif, The ADD System - An Architecture for Distributed Databases, Proc. of the 4th International Conference of Very Large Data Bases, Berlin, September1978
- S.A. Mahmoud & K.C. Toth, Design Considerations for a Mini-Computer Database, MIMI International Conference, Zurich, June 7-9, 1977
- S.A. Mahmoud, J.S. Riordon & K.C. Toth, Design of a Distributed Database File Manager for a Mini-Computer Network, COMPSAC77, Chicago, November 8-11, 1977
- Kalman C. Toth, Contributions to the Synthesis of Computer-Communication Networks, M.Eng. Thesis, Carleton University, Ottawa, April 1972

Trade Articles

- "What's the hard part of software development anyway?", Software Assoc. of Oregon, Nov. 2007
- "Better Mileage with Hybrid Learning", with Kathy Milhauser, Software Assoc. of Oregon, June 2007
- "Can Software Engineers Develop Communications Skills Online?", Software Assoc. of Oregon, March 2007
- "Is Online Software Engineering Education for You?", Software Association of Oregon (SAO), Feb 2007
- "OMSE Exchange: A Software Engineering Clearing House", Software Assoc. of Oregon (SAO), Nov 2006
- "So Many Engineering Practices: Which to Follow?" (Part III), Software Assoc. of Oregon (SAO), July 2005
- "So Many Engineering Practices: Which to Follow?" (Part II),, Software Assoc. of Oregon (SAO), June 2005
- "So Many Engineering Practices: Which to Follow?" (Part I),, Software Assoc. of Oregon (SAO), May 2005
- "Which is the Right Software Process for your Problem?", Software Assoc. of Oregon (SAO), April 2005
- "Outsourcing Software Development: A Case for Effective Scope Management", SAO, March 2005
- "Why Invest in Software Engineering Education?", SAO, February 2005
- "EDI and Security", CGI Group report, Dec. 1990
- "COSICS Security Verification Plan", Intellitech report to External Affairs, December, 1988
- "Information Security Model", report to National Defence, November 15, 1988
- "Data Encryption Equipment Specification", Internal report specifying the components of CryptoNet, Intellitech's X.25/DES product, 1986
- "A Survey of Integrated Project Support Environments", Report to the Department of National Defence, 1986
- "A New Implementation Strategy for Secure Operating Systems", Intellitech Report, March 1986

Industry Reports

- "Requirements for SimbaERP", report to Simba Technologies on the Requirements for a proposed ERP/Data Warehousing product, January, 1999
- System Security and Recovery Procedures, Datalink Systems Corp, January 1999
- "Technology Skills Gap Analysis: B.C. Software Industry", under contract to the Software Development Centre (B.C.) for B.C. Ministry of Education, Skills & Training, and National Research Council, March 1997
- "Process Product Standard", internal Hughes System Division Report, June 1994
- "In-Process Review (IPR) Process", internal Hughes System Division Report, December 1993
- "Change in Development Methodology", internal Hughes Systems Division Report, June 1, 1993
- "Total Quality Implementation Program", internal CGI report to the Management Committee, 1991
- "Total Quality Process: Directions & Priorities", internal CGI report to the Management Committee, 1991
- "TQP: Client Satisfaction Assessment Process", internal CGI guide, 1991
- "Software Quality Assurance Program", internal CGI practice guide, 1990
- "Configuration Management Framework", internal CGI practice guide, 1990
- "EDI and Security", CGI Group report, Dec. 1990
- "COSICS Security Verification Plan", Intellitech report to External Affairs, December, 1988
- "Information Security Model", report to National Defence, November 15, 1988
- "Network Processing Strategy Study", a series of reports to Transport Canada, 1988
- "Data Encryption Equipment Specification", Internal report specifying the components of CryptoNet, Intellitech's X.25/DES product, 1986
- "A Survey of Integrated Project Support Environments", Report to the Department of National Defence, 1986
- "A New Implementation Strategy for Secure Operating Systems", Intellitech Report, March 1986
- "Computer System Study" (Computer Integrated Manufacturing and Manufacturing Requirements Planning), Reports to General Metals Co, El Naser Glass Co. and Delta Steel Mills, 1985/86
- "Search and Rescue Satellite (SARSAT) Aided Tracking System, Ground System Study", five reports regarding Mission Control Centre design to National Defence, 1983 and 1984
- "Design Specification for the NCCS Communications Management System", Atmospheric Env. Serv, Jan 84
- "Design & Analysis of Alternatives for the Integrated Data Network", Report to the Dept. Nat'l Defence, 1982
- "Recovery Mechanisms for the ADD Distributed Database System", Intellitech Report, July 1982 (also presented at a NATO workshop in 1982)
- "Implementation Alternatives and Gateway Considerations for a Data Network to Serve the Defence Research Establishments", Report to the Department of National Defence, 1981
- "Design and Security Considerations for a Gateway to Interconnect SAMSON and DATAPAC", Report to the Department of National Defence, 1980
- "Open System Interconnection: Application Issues Associated with the ISO and CCITT Layered Models", report to the Department of Communications, 1980
- "On Query Decomposition & Processing in Distributed DBs", INRIA Research Report, Spyratos & Toth, 1980
- "Query Processing Strategy Formulation in ADD", Carleton University report, 1979
- "A Modeling Approach to Systems Analysis of Processing Networks", one of five reports to the Department of Communications, Spectrum Management Systems
- "Design Issues in Distributed Databases", Carleton University report
- "Design & Configuration Analysis of an Aeronautical Satellite Comm. Centre (ASCC)", Transport Canada

Workshops, Seminars, Tutorials, Professional Training Courses

- Professional Development Course in Software Engineering for Regence Group, Portland, Or, June 2007
- "Identity Management Systems", tutorial for IEEE International Computer Software and Applications Conference (COMPSAC), Chicago, September 2006
- Information security seminars for the Assoc. of Prof. Engineers and Geoscientists of B.C., 2002 and 2006
- Extending the Reach of Mobile E-Commerce, Software Productivity Centre, June 2000
- Wireless Handheld Technologies and Telelearning, Telelearning Conference, Toronto, November 2000
- E-Commerce Lifecycle, Transactions and Security, MacDonald Dettwiler & Assoc., November 1999
- Personal Software Process (PSP): Software Productivity Centre / MacDonald Dettwiler & Associates, 1997
- WestMOST Software Engineering Telelearning Workshop, Saskatoon, 1998
- Software Project Management (including software process and metrics) at Carleton University, Dec 1994
- Software Development Methods and Process: Iterative Software Development, for the Canadian Automated Air Traffic System (CAATS) at Hughes Aircraft, Systems Division and Transport Canada, March 1993
- Canadian Automated Air Traffic System, seminars presented at UBC (Computer Science), SFU (Applied Sciences), and Hughes (for staff and graduate students from UVIC, BCIT, SFU and UBC), 1993 and 1994
- Total Quality Management, seminars presented to CGI Group technical staff across Canada,1991 and 1992
- Total Quality Management, lecture to 4th year computer systems engineers at Carleton University, 1991
- Information Security Technology Overview for AFCEA INFOSEC Course, Canadian Forces Base (CFB) Kingston, October 1991

University Undergraduate and Graduate Courses

For Portland State University:

- Principles of Software Engineering
- Software Project Management
- Software Quality Engineering
- Software Design Techniques
- Software Estimating
- Distributed Software Engineering Team Collaboration
- Software Engineering Practicum
- Computing Fundamentals II (Visual Basic)
- Senior Capstone projects
- Directed studies: IT and software engineering

For Oregon State University:

- E-Commerce Systems
- Software Engineering I: principles, processes, requirements, OO design, architecture, SPM
- Software Engineering II: implementation, SCM, test techniques, reviews and inspections, SQA

For the Technical University of British Columbia and the University of Alberta:

- Software Engineering Best Practices
- E-Commerce Systems

For the University of British Columbia and Simon Fraser University:

- Software Engineering Best Practices
- Software Project Management
- Professional Issues in Software Engineering
- Software Engineering Team Project

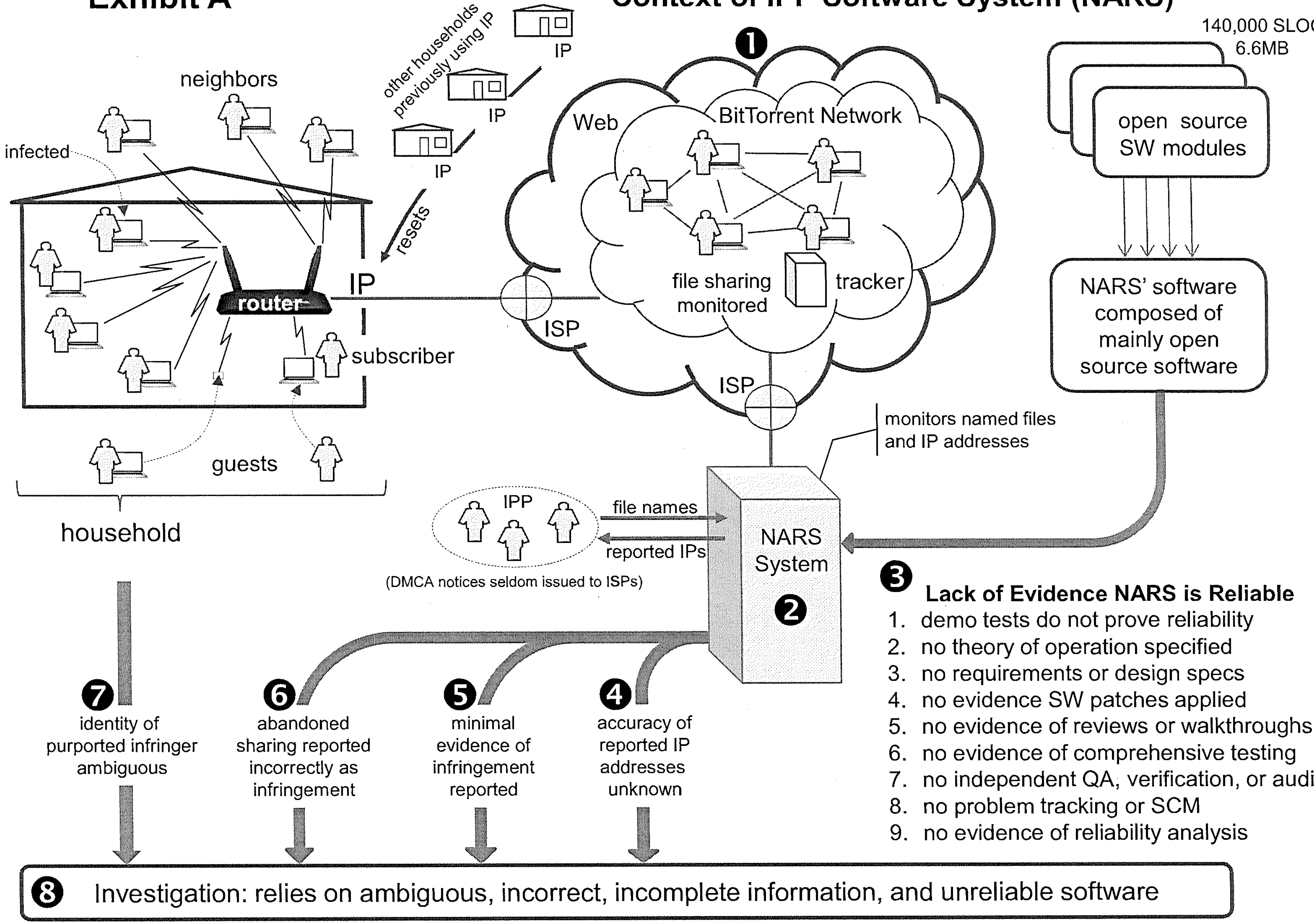
For Carleton University:

- Undergrad course on data structures, databases, programming, and computer architecture

Exhibit A: Context

Exhibit A

Context of IPP Software System (NARS)

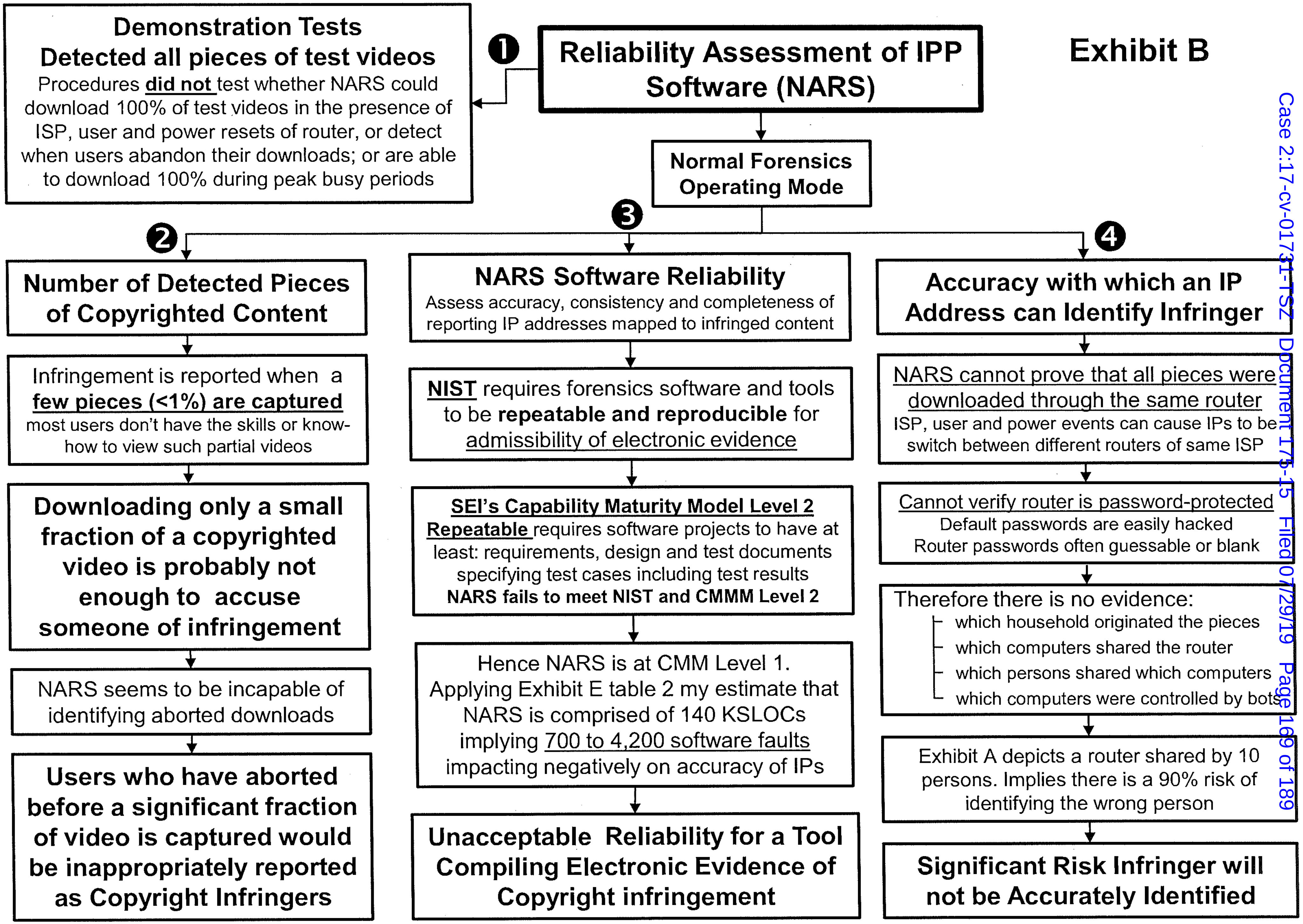

neighbors
infected
other households previously using IP
IP
IP
IP
resets
IP
router
subscriber
guests
household
❶
Web
BitTorrent Network
file sharing monitored
tracker
ISP
ISP
140,000 SLOC
6.6MB
open source SW modules
NARS' software composed of mainly open source software
monitors named files and IP addresses
IPP
file names
reported IPs
(DMCA notices seldom issued to ISPs)
NARS System
❷
❹ accuracy of reported IP addresses unknown
❺ minimal evidence of infringement reported
❻ abandoned sharing reported incorrectly as infringement
❼ identity of purported infringer ambiguous
❽ Investigation: relies on ambiguous, incorrect, incomplete information, and unreliable software

❸ **Lack of Evidence NARS is Reliable**

1. demo tests do not prove reliability
2. no theory of operation specified
3. no requirements or design specs
4. no evidence SW patches applied
5. no evidence of reviews or walkthroughs
6. no evidence of comprehensive testing
7. no independent QA, verification, or audits
8. no problem tracking or SCM
9. no evidence of reliability analysis

Exhibit B: Reliability Assessment

Exhibit B



Reliability Assessment of IPP Software (NARS)

❶

Demonstration Tests

Detected all pieces of test videos

Procedures **did not** test whether NARS could download 100% of test videos in the presence of ISP, user and power resets of router, or detect when users abandon their downloads; or are able to download 100% during peak busy periods

Normal Forensics Operating Mode

❷

Number of Detected Pieces of Copyrighted Content

Infringement is reported when a **few pieces (<1%) are captured**

most users don't have the skills or know-how to view such partial videos

Downloading only a small fraction of a copyrighted video is probably not enough to accuse someone of infringement

NARS seems to be incapable of identifying aborted downloads

Users who have aborted before a significant fraction of video is captured would be inappropriately reported as Copyright Infringers

❸

NARS Software Reliability

Assess accuracy, consistency and completeness of reporting IP addresses mapped to infringed content

NIST requires forensics software and tools to be **repeatable and reproducible** for admissibility of electronic evidence

SEI's Capability Maturity Model Level 2

Repeatable requires software projects to have at least: requirements, design and test documents specifying test cases including test results

NARS fails to meet NIST and CMMM Level 2

Hence NARS is at CMM Level 1.

Applying Exhibit E table 2 my estimate that NARS is comprised of 140 KSLOCs implying 700 to 4,200 software faults impacting negatively on accuracy of IPs

Unacceptable Reliability for a Tool Compiling Electronic Evidence of Copyright infringement

❹

Accuracy with which an IP Address can Identify Infringer

NARS cannot prove that all pieces were downloaded through the same router

ISP, user and power events can cause IPs to be switch between different routers of same ISP

Cannot verify router is password-protected

Default passwords are easily hacked

Router passwords often guessable or blank

Therefore there is no evidence:

- which household originated the pieces
- which computers shared the router
- which persons shared which computers
- which computers were controlled by bots

Exhibit A depicts a router shared by 10 persons. Implies there is a 90% risk of identifying the wrong person

Significant Risk Infringer will not be Accurately Identified

Exhibit C: BitStalker Article

BITSTALKER: ACCURATELY AND EFFICIENTLY MONITORING BITTORRENT TRAFFIC

Kevin Bauer, Damon McCoy, Dirk Grunwald, and Douglas Sicker

University of Colorado, Boulder, CO, USA
{bauerk, mccoyd, grunwald, sicker}@colorado.edu

ABSTRACT

BitTorrent is currently the most popular peer-to-peer network for file sharing. However, experience has shown that BitTorrent is often used to distribute copyright protected movie and music files illegally. Consequently, copyright enforcement agencies currently monitor BitTorrent swarms to identify users participating in the illegal distribution of copyright-protected files. These investigations rely on passive methods that are prone to a variety of errors, particularly false positive identification.

To mitigate the potential for false positive peer identification, we investigate the feasibility of using *active* methods to monitor extremely large BitTorrent swarms. We develop an active probing framework called *BitStalker* that identifies active peers and collects concrete forensic evidence that they were involved in sharing a particular file. We evaluate the effectiveness of this approach through a measurement study with real, large torrents consisting of over 186,000 peers. We find that the current investigative methods produce at least 11% false positives, while we show that false positives are rare with our active approach.

Index Terms— Data mining for forensic evidence

1. INTRODUCTION

While BitTorrent provides the ability to transfer files among many users quickly and efficiently, experience has shown that its decentralized architecture also makes it appealing for sharing copyright protected files illegally. With a peer-to-peer network like BitTorrent, content is distributed and replicated among a potentially large set of peers, making the process of finding and contacting each peer hosting the content in question a difficult task. Despite the challenge, entities acting on behalf of copyright holders have begun to monitor BitTorrent file transfers on a massive scale to identify and contact users who violate copyright laws.

In fact, a recent study [1] shows how the entities representing copyright holders use naïve techniques such as querying the BitTorrent tracker servers to identify individual users participating in an illegal file transfer. After being identified, these entities often distribute DMCA take-down notices or even pursue more formal legal sanctions against individuals who appear in the tracker's peer list. However, this simple approach is prone to a wide variety of errors. For instance, it is trivial to introduce erroneous information into the tracker lists by explicitly registering fake hosts to the tracker. The authors of the recent study demonstrate this type of false positive identification by registering networked devices such as printers and wireless access points to tracker lists and subsequently receiving DMCA take-down notices for their suspected participation in illegal file transfers.

This strategy of polluting tracker lists with fake peers could be used to frustrate anti-piracy investigations. The Pirate Bay, a popular tracker hosting site, has allegedly begun to inject arbitrary, but valid IP addresses into their tracker lists [2]. This counter-strategy may further increase the potential for false positive identification, which could have serious consequences as this evidence can be used to initiate legal action against suspected file sharers.

Given the inaccurate nature of the current techniques for monitoring BitTorrent file transfers and the clear need for effective anti-piracy tactics, we consider this question: Is it feasible to develop and deploy an efficient technique for identifying and monitoring peers engaged in file sharing that is more accurate than querying the trackers?

To answer this question, we propose a technique that is active, yet efficient. Starting with the tracker's peer lists, each peer listed by the tracker server is actively probed to confirm their participation in the file sharing and to collect concrete forensic evidence. Our tool, called BitStalker, issues a series of lightweight probes that provide increasingly conclusive evidence for the peers' active participation in the file sharing.

To evaluate the feasibility of this active approach in practice, we conduct a measurement study with real, large torrents. In particular, we quantify the number of peers that can be identified, the potential for falsely identifying peers, the potential for missing peers, and the cost associated with this technique in terms of bandwidth. Our results indicate that active probing can identify a sufficiently large portion of the active peers while requiring only 14.4–50.8 KB/s and about five minutes to monitor over 20,000 peers (using a commodity desktop machine). We also show that the active probing can be parallelized and scale to monitor millions of peers inexpensively using cloud computing resources such as Amazon's Elastic Compute Cloud (EC2) [3]. Using EC2, we estimate that our method can monitor the entire Pirate Bay (about 20 million peers) for only $12.40 (USD).

2. BACKGROUND

Before we describe our method for monitoring large BitTorrent swarms, we first provide a description of the BitTorrent protocol and an overview of the techniques currently being applied to identify peers who are sharing a file with BitTorrent.

2.1. The BitTorrent Protocol

To share a file, BitTorrent first breaks the file into several fixed size *pieces* and computes a SHA1 hash of each piece to verify integrity. Pieces are sub-divided into smaller data units called *blocks*, typically 16 KB in size. A metadata file containing the SHA1 hashes for each piece along with other information necessary to download the file including a URI to the *tracker server* is distributed to interested users via an out-of-band mechanism. Once a user has obtained the metadata for a file of interest, they proceed by contacting the tracker server to obtain a randomly chosen subset of peers who are sharing

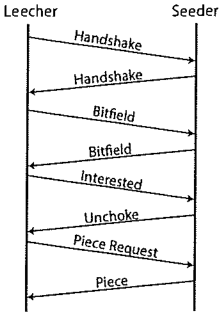


Fig. 1. BitTorrent message exchange to start a piece transfer

the file. This is called the *peer list*. By obtaining a peer list from the tracker (or another distributed hash table-based or gossip-based mechanism), the peer also registers itself with the tracker. The peer then begins requesting blocks of the file. Peers that are downloading pieces of the file are called "leechers," while peers that possess all pieces and participate as uploaders are referred to as "seeders."

The precise sequence of messages involved in the request of pieces is shown in Figure 1. A leecher establishes communication with another peer by exchanging `handshake` messages. The handshake consists of a plain text protocol identifier string, a SHA1 hash that identifies the file(s) being shared, and a peer identification field. After the handshake exchange, the leecher transmits a `bitfield` message. This contains a bit-string data structure that compactly describes the pieces that the peer has already obtained. After exchanging bitfields, the leecher knows which pieces the other peer can offer, and proceeds to request specific blocks of the file. The leecher sends an `interested` message to notify the other peer that it would like to download pieces. The other peer responds with an `unchoke` message only if it is willing to share pieces with the leecher. Upon receiving an unchoke message, the leecher asks for specific blocks of the file.

2.2. BitTorrent Monitoring Practices

While BitTorrent provides an efficient way to distribute data to a large group of users, it is also an appealing technique to distribute copyright protected files illegally. Copyright enforcement is particularly challenging within the context of BitTorrent, since the file(s) in question are distributed among a set of arbitrarily many peers. The copyright holders must first *identify* every user who appears to be sharing the file and ask them to stop sharing.

Despite the significant amount of work required to monitor BitTorrent networks, a recent study has gathered evidence showing that investigative entities acting on behalf of various copyright holders are monitoring and tracking BitTorrent users who are suspected of sharing copyright protected files [1]. These investigators — including BayTSP [4], Media Defender [5], and Safenet [6] who are hired by organizations such as the Motion Picture Association of America (MPAA) and the Recording Industry Association of America (RIAA) — are using *passive* techniques, such as querying the trackers for the peer lists to identify users who are engaged in illegal file sharing. Once a list of peers has been obtained, an ICMP echo (ping) message is sent to each IP address to ensure that it is alive.

However, as the aforementioned study notes, these methods for monitoring large BitTorrent networks can be wildly inaccurate. For instance, it is possible to implicate arbitrary networked devices by simply registering their IP addresses with the tracker server. In addition, *false positive* identification is also possible as a result of naturally occurring (*i.e.*, non-intentional) activity. For instance, the tracker may provide stale peer information, which may result in a user who recently obtained a DHCP lease on an IP address being implicated in the file sharing. The very real potential for false positives could have serious implications, since the investigators who conduct this monitoring often issue DMCA take-down notices or even initiate legal actions against the suspected file sharers.

3. ACCURATE AND EFFICIENT MONITORING

In order to study the feasibility of collecting forensic evidence to concretely prove a peer's participation in file sharing, we present *BitStalker*. BitStalker is active, yet efficient, since it consists of small probe messages intended to identify whether a peer is actively engaged in a file transfer. First, to obtain the list of peers who are potentially sharing the file, the tracker is queried. For each IP address and port number returned, we conduct a series of light-weight probes to determine more conclusively whether the peer really exists and is participating in the file transfer.

TCP connection. The first probe consists of an attempt to open a TCP connection to the IP address on the port number advertised by the tracker. A successful TCP connection indicates that the suspected peer is listening for connections on the correct port.

Handshake. If a TCP connection is established, a valid BitTorrent handshake message is sent. If the handshake succeeds, then the investigator has obtained evidence that the suspected peer is responding to the BitTorrent protocol, and may even provide information about the BitTorrent client software being used.

Bitfield. If the handshake probe succeeds, then a BitTorrent bitfield message is sent. This message contains a concise representation of all pieces that have been downloaded by the peer. A random bitfield is generated so that the probe looks like a valid bitfield message. If a peer responds with a valid bitfield message, then the investigator has obtained evidence that the peer has downloaded the part of the file that is described by their bitfield. This also indicates whether the peer is a seeder or a leecher. This provides the strongest form of forensic evidence that the peer is actively sharing the file without exchanging file data.

Block request. If the bitfield probe succeeds, we finally attempt to request a 16 KB block of the file from the peer. First, the peer's bitfield is examined to find a piece of the file that the peer has obtained. Next, this probe sends an interested message to indicate that we want to exchange pieces with this peer. The peer responds with an unchoke message, which implies that we are allowed to ask for pieces. We finally request a 16 KB block. If the peer responds with the block requested, then this probe succeeds. A single block is the smallest amount of data necessary to confirm that another peer is sharing the file. If the investigator has the remaining blocks of that piece, then they can verify the hash to ensure that the block is valid.

We argue that each probe type provides increasingly conclusive evidence of a peer's active involvement in file sharing. A successful TCP probe indicates that the peer is listening on the correct port. However, an effective counter-strategy could be to register arbitrary IP addresses with ports that are opened (such as web servers). The subsequent handshake probe is more conclusive, as it indicates that the BitTorrent protocol

Table 1. Summary of data sources

Torrent ID	Total Peers	Media Type
1	20,354	TV Series
2	16,979	TV Series
3	11,346	TV Series
4	14,691	TV Series
5	23,346	Movie
6	20,777	TV Series
7	24,745	TV Series
8	13,560	TV Series
9	19,694	TV Series
10	20,611	Movie
Total:	186,103	

is running on the correct port and also identifies the content being shared by a SHA1 hash. The bitfield probe provides stronger evidence still, since it describes all pieces that the peer has downloaded, which implies active sharing. Finally, requesting and subsequently receiving a block of the file provides the strongest form of concrete evidence for file sharing.

Practical considerations. The active probing framework can monitor peers who are actively participating in the file sharing. However, if a peer has just joined the torrent when they are probed, then they may not have any pieces of the file yet. Consequently, according to the BitTorrent protocol, if a peer has no pieces, then the bitfield probe is optional. Since the peer has not yet obtained any pieces of the file, the probing does not collect any evidence from this peer. If peers are probed repeatedly over time, then the likelihood of this case becomes negligible.

Additionally, "super-seeding" mode is enabled when a torrent is first established and there are few seeders. Super-seeding mode ensures that the original seeder is not overwhelmed by piece requests from other peers before it transfers data to another peer. When super-seeding is activated, the seeder may advertise an empty or modified bitfield, even though they possess every piece. Since we are interested in monitoring mature torrents consisting of at least tens of thousands of peers, we disregard new torrents in super-seeder mode.

Lastly, it is possible that peers may be able to detect the monitors and blacklist them. Siganos *et al.* show that the current passive BitTorrent monitors can be detected by observing that the frequency with which the monitor's IP addresses occur across a large number of tracker lists is statistically higher than that of normal peers [7]. Our active monitoring may also be identifiable in the same manner. To address this, we recommend that the monitoring be distributed across a large number or dynamic set of IP addresses.

4. EXPERIMENTAL EVALUATION

In this section, we present experiments to quantify both the effectiveness and the cost of monitoring large BitTorrent swarms using the active probing technique. In addition, we compare the accuracy, potential for false positives and false negatives, and the cost with the current strategy employed widely by anti-piracy investigators.

4.1. Data Sources and Methodology

To evaluate our light-weight probing technique, we selected ten large torrents each containing between 11,346 and 24,745 unique peers. In total, our experimental evaluation consists of over 186,000 peers. Peers participating in these torrents were sharing new theatrical releases and episodes of popular television shows (summarized in Table 1). These swarms represent the type of file sharing that may be monitored by copyright enforcement agencies.

To conduct the active probing, we wrote a tool called BitStalker that can perform the following tasks:

- Establish a TCP connection with another peer
- Exchange handshake messages with the correct SHA1 content hash and receive handshake responses
- Exchange bitfield messages and receive bitfield responses
- Request and receive a 16 KB block of file data

In short, BitStalker efficiently probes for participation in the BitTorrent protocol by sending and receiving a minimal number of small control messages rather than downloading the entire file from other peers.

The experiments were conducted as follows: The tracker server is contacted to obtain a subset of the peers who are currently believed to be sharing the file. Since the trackers only return a randomly selected set of 100 peers, it is necessary to query the tracker several times to obtain a large portion of the hosts registered with the tracker. Once peers are obtained from the tracker, BitStalker attempts to establish a TCP connection with each peer on its advertised TCP port. If a connection is established, a handshake message exchange is attempted. If handshake messages are exchanged, BitStalker attempts to exchange bitfield messages. Finally, if bitfields are exchanged, the tool attempts to retrieve a single block of the file. This procedure is repeated for each torrent to be monitored.

We compare our active probing method with the current approach to peer identification described in Section 2.2. After obtaining the list of suspected peers from the tracker, our tool sends precisely five ICMP echo (ping) messages to each IP address in the peer list. If a host responds to at least one ping, then it is assumed (perhaps erroneously) to be alive and sharing the file.

4.2. Experimental Results

We evaluate the proposed peer probing technique with regard to the number of peers that can be identified, an estimate of the number of peers that are falsely identified as being a file sharer (false positives), an estimate of the number of peers that this technique fails to identify (false negatives), and the measured cost of performing this active probing. The probing mechanism is compared along each of these metrics to the passive identification process using ping messages to verify the tracker's peer list.

Fraction of peers that respond. We first consider how many peers can be identified by active probing. As shown in Table 2, the fraction of peers that can be positively identified by each probe type increases with additional repetitions. To determine if additional peers can be identified through multiple probing attempts, the experiments are repeated ten times. Even though the number of peers probed remains constant for each repetition, we find that the fraction of peers that respond to probes increases, since some peers may be busy interacting with other peers when we probe.

The complete results for each torrent are given in Figure 2. Across the ten torrents, we could establish a TCP connection with between 26.7–44.6% of the peers listed by the tracker. While this percentage seems low, it is reasonable since many BitTorrent clients impose artificial limits on the number of open connections allowed, in order to reduce the amount of bandwidth consumed. A similar fraction of peers that establish connections is reported by Dhungel *et al.* [8].

The naïve ping method returns roughly the same fraction of peers as the active TCP connection probe. However, as we

Table 2. The average fraction of peers identified in one, five, and ten iterations of the monitoring across all ten torrents

Repetitions	Connection	Handshake	Bitfield	Block Request
1	30.8%	18.9%	17.7%	0.29%
5	35.9%	26.3%	25.3%	0.80%
10	36.9%	28.4%	27.6%	1.13%

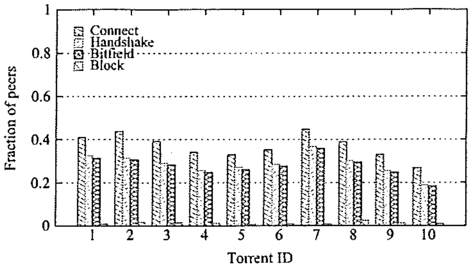


Fig. 2. Over ten runs, the cumulative fraction of peers identified with connections, handshakes, bitfields, and block requests across all ten torrents

will show, the ping probes are susceptible to an intolerably high number of false positives, while active probing significantly reduces the potential for false positives.

Both the handshake and bitfield probes succeed for between 18.6–36.6% of the peers. While this is lower than the TCP connection probe, it provides significantly stronger evidence for file sharing. For this fraction of the peers, an investigator can tell that the peer is obeying the BitTorrent protocol, sharing the correct file identified in the handshake probe by a SHA1 hash, and advertising the pieces of the file that the peer already possesses as identified in the bitfield probe. We argue that this small reduction in the fraction of peers that respond to bitfield probes is a small price for greater confidence in the identification results.

Finally, we observe that block request probes succeed for a very small faction of the peers, only 0.6–2.4%. This may be partly a result of BitTorrent's tit-for-tat incentive mechanism [9], which attempts to mitigate selfish leechers by enforcing reciprocity in the piece request process. This is implemented by uploading to other leechers from whom you download. The leecher with the highest upload rate receives download priority. Since BitStalker has a zero upload rate, it does not receive priority for piece requests. However, BitTorrent does offer optimistic unchoking, which enables a leecher to download regardless of their upload rate. BitStalker only receives pieces from other peers who have chosen to optimistically unchoke.[1] Since only about 1% of the peers respond to our block requests on average, we argue that the minimal additional evidence obtained through this probe is not worth the extra time and bandwidth required to collect this evidence.

False positives. The most serious flaw with the past and present investigative tactics based on tracker list queries and ping probes is the real potential for a high number of false positives. Furthermore, active peer list pollution further increases the potential for false positives.

To establish a lower bound on false positives obtained by the naïve investigative strategy, we count the number of peers that respond to pings yet show no indication of running any network service on their advertised port. More technically, if a peer responds to a TCP SYN request with a TCP RST (reset) packet, this indicates that the remote machine exists, but it is not running any service on the advertised TCP port. From our experiments, we observe that 11% of peers exhibit this behavior on average and are, therefore, definite false positives using this naïve investigative strategy.

In addition, we count the number of peers that *could* be false positives with the ping method. These are the peers that respond to ping probes, but ignore the TCP probe (*i.e.*, no connection or reset packet). From our experiments, we find that on average an additional 25.7% of the peers could potentially be false positives, but we cannot say this conclusively. It's possible that some of these peers could have reached a connection limit in their BitTorrent client or could be filtering incoming traffic.

In contrast to the naïve ping method, the active probing strategy offers more reliable peer identification with few avenues for false positives. For instance, a successful TCP probe indicates that the peer is listening for connections on its advertised port. However, one could envision a more intelligent pollution strategy where arbitrary IP addresses with open ports are inserted into trackers (*i.e.*, real HTTP or FTP servers). The subsequent handshake and bitfield probes would then eliminate this form of pollution by checking that the host is running the BitTorrent protocol.

However, the active probing approach is not entirely immune from the possibility of false positive identification. For example, peers using an anonymizing network such as Tor [10] may produce false positives, since the last Tor router on the client's path of Tor routers (called a Tor exit router) would be implicated in the file sharing. In fact, a recent study has found that BitTorrent is among the most common applications used with Tor [11].

To determine how common this type of false positive is in practice, we compare the list of potential BitTorrent peers obtained through our experiments to the list of all known Tor exit routers provided by Tor's public directory servers. On average, we find that only approximately 1.8% of the peers are using Tor to hide their identities.[2] However, these are not false positives using active probing, since a peer using Tor (or another anonymizing network or proxy service) cannot bind to the advertised port on the exit host to accept incoming connections. Consequently, active probing does not provide any evidence for these peers. Furthermore, peers using Tor are easily identifiable and can be filtered out of the results.

In addition to general-purpose anonymizing networks, solutions have been proposed specifically for anonymizing BitTorrent. For instance, SwarmScreen's goal is to obscure a peer's file sharing habits by participating in a set of random file sharing swarms [12]. Also, BitBlender attempts to provide plausible deniability for peers listed by the trackers by introducing relay peers that do not actively share files, but rather act as proxies for other peers actively sharing the file [13]. The active methods we propose would identify peers utilizing SwarmScreen and BitBlender as file sharers. While these peers are not intently sharing content, an investigator may still be interested in pursuing these peers since they contribute pieces of the file to other peers who are actively sharing.

False negatives. False negative identification occurs when a peer who is actively sharing a file cannot be identified as a file sharer. Both the active probing technique and the naïve ping method suffer from the potential for false negatives. The ping method may miss peers who are behind a firewall that blocks incoming ICMP traffic. For example, this is the default configuration for Windows Vista's firewall settings. The active probing method may also suffer from false negatives when a

[1] Additional blocks may be received if BitStalker offered blocks before asking for blocks.

[2] However, several peers could be using each of these Tor exit nodes.

Table 3. Size of each probe type (assuming no TCP options)

Probe Type	Description	Size
TCP connection	Three-way handshake	162 Bytes
Handshake	Handshake request/reply	244 Bytes
Bitfield	Bitfield request/reply	Variable
Block Request	Block request/reply	16.688 KBytes
ICMP Ping	Ping request/reply	86 Bytes

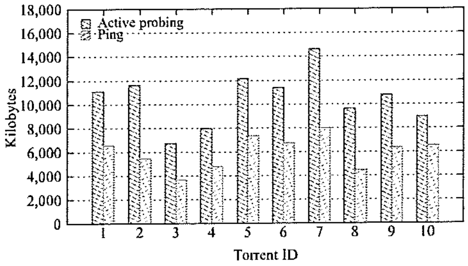


Fig. 3. Total amount of traffic necessary to monitor each torrent using active probing and pings

peer's number of allowed connections is at the maximum. In this case, the initial TCP connection probe will fail to identify that the peer is listening on its advertised port. In general, we found that repeating the monitoring procedure decreases false negatives. Table 2 shows that the number of false negatives decreases as the experiment is repeated. Although there are diminishing returns, as the false negatives do not decrease significantly between 5 and 10 iterations of the monitoring.

We can, however, provide a lower bound on false negatives obtained with the naïve ping method. This is achieved by counting the number of peers that do not respond to pings, but do respond to the TCP connection probe. Our experiments show that the naïve ping method would fail to identify at least 22.3% of the peers on average.

Cost. In order for an active probing strategy to be a feasible technique to monitor large BitTorrent swarms in practice, it is necessary for the probing to be as efficient as possible. Table 3 shows that the size of each probe is small and Figure 3 shows the amount of traffic that was required to monitor each torrent using the active probing technique. For comparison, the cost for the ping method is also plotted. While the ping approach requires less bandwidth, we have shown that it is not sufficiently accurate in identifying active file sharers. Using a modest Linux desktop machine, it took 304.5 seconds on average to monitor an entire torrent, which required only 14.4–50.8 KB/s of bandwidth. The active probing overhead is dependent on the fraction of peers that respond to active probes. This is an intuitive result, implying a direct relationship between the number of peers identified and the amount of bandwidth required by the probing.

The active probing method is also highly scalable, particularly when inexpensive cloud computing resources such as Amazon's Elastic Compute Cloud (EC2) [3] are utilized. Machines from EC2 are available at a small cost dependent on the execution time and bandwidth usage of the jobs. From our experiments, on average we probed approximately 61 peers/second, uploaded 288.2 bytes/peer and downloaded 296.6 bytes/peer. Using EC2's pricing model, we estimate that it is possible to monitor peers at an expected cost of roughly 13.6 cents/hour (USD). In fact, it's possible to scale the active probing to monitor the entire Pirate Bay, which claims to track over 20 million peers [14]. We estimate that this method can monitor the Pirate Bay for $12.40 (USD).

5. CONCLUSION

This paper presents *BitStalker*, a low-cost approach to monitoring large BitTorrent file sharing swarms. BitStalker collects concrete evidence of peers' participation in file sharing in a way that is robust to tracker pollution, highly accurate, and efficient. In contrast, the past and present investigative monitoring strategy consists of tracker server queries and ICMP ping probes. While this method is simple, it is also prone to a variety of significant errors, especially false positive identification, since this monitoring technique does not verify participation in the file sharing. We present an alternative monitoring strategy based on actively probing the list of suspected peers to obtain *more conclusive* evidence of participation in the file sharing.

There are several aspects of our approach that warrant additional attention. In particular, a specific definition of what constitutes "evidence" in the context of file sharing across various legal systems should be explored. Also, the general legal issues that this type of monitoring exposes should also be investigated further.

Acknowledgments. The authors thank the anonymous reviewers for their valuable comments and suggestions. We also thank Claire Dunne and the University of Colorado's institutional review board for ensuring that this research was conducted with the highest of ethical standards. This research was funded in part through gifts from PolyCipher.

6. REFERENCES

[1] Michael Piatek, Tadayoshi Kohno, and Arvind Krishnamurthy, "Challenges and directions for monitoring P2P file sharing networks – or – Why my printer received a DMCA takedown notice," in *3rd USENIX Workshop on Hot Topics in Security (HotSec)*, July 2008.

[2] "Pirate bay tricks anti-pirates with fake peers," http://torrentfreak.com/the-pirate-bay-tricks-anti-pirates-with-fake-peers-081020.

[3] "Amazon elastic compute cloud (amazon ec2)," http://aws.amazon.com/ec2.

[4] "BayTSP," http://www.baytsp.com.

[5] "Media defender – P2P anti-piracy and P2P marketing solutions," http://www.mediadefender.com.

[6] "Safenet Inc: The foundation for information security," http://www.safenet-inc.com.

[7] Georgos Siganos, Josep M. Pujol, and Pablo Rodriguez, "Monitoring the Bittorrent monitors: A bird's eye view," in *PAM*, 2009, pp. 175–184.

[8] Prithula Dhungel, Di Wu, Brad Schonhorst, and Keith W. Ross, "A measurement study of attacks on bittorrent leechers," in *International Workshop on Peer-to-Peer Systems (IPTPS)*, February 2008.

[9] "BitTorrent protocol specification," http://wiki.theory.org/BitTorrentSpecification.

[10] Roger Dingledine, Nick Mathewson, and Paul Syverson, "Tor: The second-generation onion router," in *Proceedings of the 13th USENIX Security Symposium*, August 2004.

[11] Damon McCoy, Kevin Bauer, Dirk Grunwald, Tadayoshi Kohno, and Douglas Sicker, "Shining light in dark places: Understanding the Tor network," in *Proceedings of the 8th Privacy Enhancing Technologies Symposium*, July 2008.

[12] David R. Choffnes, Jordi Duch, Dean Malmgren, Roger Guierma, Fabian E. Bustamante, and Luis Amaral, "SwarmScreen: Privacy through plausible deniability for P2P systems," Northwestern EECS Technical Report, March 2009.

[13] Kevin Bauer, Damon McCoy, Dirk Grunwald, and Douglas Sicker, "BitBlender: Light-weight anonymity for BitTorrent," in *Proceedings of the Workshop on Applications of Private and Anonymous Communications (AlPACa 2008)*, Istanbul, Turkey, September 2008, ACM.

[14] "The pirate bay," http://thepiratebay.org.

Exhibit D: Validation of Forensics Tools and Software

Validation of Forensic Tools and Software: A Quick Guide for the Digital Forensic Examiner

Wed, 03/02/2011 - 7:45am by Josh Brunty

With the field of digital forensics growing at an almost warp-like speed, there are many issues out there that can disrupt and discredit even the most experienced forensic examiner. One of the issues that continues to be of utmost importance is the validation of the technology and software associated with performing a digital forensic examination. The science of digital forensics is founded on the principles of repeatable processes and quality evidence. Knowing how to design and properly maintain a good

Tools and software for digital forensic analysis should be validated quarterly.

DEEPER INSIGHTS

The Importance of Mobile Forensics for Law Enforcement

Forensic

validation process is a key requirement for any digital forensic examiner. This article will attempt to outline the issues faced when drafting tool and software validations, the legal standards that should be followed when drafting validations, and a quick overview of what should be included in every validation.

Setting the Standard: Standards and Legal Baselines for Software/Tool Validation

According to the National Institute of Standards and Technology (NIST), test results must be *repeatable* and *reproducible* to be considered admissible as electronic evidence. Digital forensics test results are repeatable when the same results are obtained using the same methods in the same testing environment. Digital forensics test results are reproducible when the same test results are obtained using the same method in a different testing environment (different mobile phone, hard drive, and so on). NIST specifically defines these terms as follows:

Repeatability refers to obtaining the same results when using the same method on identical test items in the same laboratory by the same operator using the same equipment within short intervals of time.

Reproducibility refers to obtaining the same results being obtained when using the same method on identical test items in different laboratories with different operators utilizing different equipment.

In the legal community, the Daubert Standard can be used for guidance when drafting software/tool validations. The Daubert Standard allows novel tests to be admitted in court, as long as certain criteria are met. According to the ruling in *Daubert v. Merrell Dow Pharmaceuticals Inc.* the following criteria were identified to determine the reliability of a particular scientific technique:

1. Has the method in question undergone empirical testing?
2. Has the method been subjected to peer review?
3. Does the method have any known or potential error rate?

4. Do standards exist for the control of the technique's operation?
5. Has the method received general acceptance in the relevant scientific community?

The Daubert Standard requires an independent judicial assessment of the reliability of the scientific test or method. This reliability assessment, however, does not require, nor does it permit, explicit identification of a relevant scientific community and an express determination of a particular degree of acceptance within that community. Additionally, the Daubert Standard was quick to point out that the fact that a theory or technique has not been subjected to peer review or has not been published does not automatically render the tool/software inadmissible. The ruling recognizes that scientific principles must be flexible and must be the product of reliable principles and methods. Although the Daubert Standard was in no way directed toward digital forensics validations, the scientific baselines and methods it suggests are a good starting point for drafting validation reports that will hold up in a court of law and the digital forensics community.

The Scientific Method and Software/Tool Validations: A Perfect Fit

In the *Daubert* ruling, The Court defined scientific methodology as "the process of formulating hypotheses and then conducting experiments to prove or falsify the hypothesis." The Scientific Method refers to a body of techniques for investigating phenomena, acquiring new knowledge, or correcting and integrating previous knowledge. To be termed scientific, the method must be based on gathering, observing, or investigating, and showing measurable and repeatable results. Most of the time, the scientific process starts with a simple question that leads to a hypothesis, which then leads to experimentation, and an ultimate conclusion. To exemplify, if you are validating a particular hardware write blocking device you may want to start with the simple question "Does this tool successfully allow normal write-block operation to occur to source media?" Since it is assumed that the write-blocking device supports various types of media (SATA, IDE, and so on) you may be required to list the various requirements of the tool. Because if this, it is good practice for an examiner to use the scientific method as a baseline for formulating digital forensic validations. It is recommended that forensic examiners follow these four basic steps as a starting point for an internal validation program:

1) Develop the Plan

Developing the scope of the plan may involve background and defining what the software or tool should do in a detailed fashion. Developing the scope of the plan also involves creating a protocol for testing by outlining the steps, tools, and requirements of such tools to be used during the test. This may include evaluation of multiple test scenarios for the same software or tool. To illustrate, if validating a particular forensic software imaging tool, that tool could be tested to determine whether or not it successfully creates, hashes, and verifies a particular baseline image that has been previously setup. There are several publically available resources and guides that can be useful in establishing what a tool should do such as those available from NIST's Computer Forensic Tool Testing Project (CFTT) available from http://www.cftt.nist.gov. The CFTT also publishes detailed validation reports on various types of forensic hardware and software ranging from mobile phones to disk imaging tools. In addition to CFTT, Marshall University has published various software and tool validation reports that are publically available for download from http://forensics.marshall.edu/Digital/Digital-Publications.html. These detailed reports can be used to get a feel for how your own internal protocol should be drafted. The scope of the plan may also include items such as: tool version, testing manufacturer, and how often the tests will be done. These factors should be established based on your organization standards. Typically, technology within a lab setting is re-validated quarterly or biannually at the very least.

2) Develop a Controlled Data Set

This area may be the longest and most difficult part of the validation process as it is the most involved. This is because it involves setting-up specific devices and baseline images and then adding data to the specific areas of the media or device. Acquisitions would then need to be performed and documented after each addition to validate the primary baseline. This baseline may include a dummy mobile phone, USB thumb drive, or hard drive depending on the software or hardware tool you are testing. In addition to building your own baseline images, Brian Carrier has posted several publically available disk images designed to test specific tool capabilities, such as the ability to recover deleted files, find keywords, and process images. These data sets are documented and are available at http://dftt.sourceforge.net. Once baseline images are created, tested, and validated it is a good idea to document what is contained within these images. This will not only assist in future validations, but may also be handy for internal competency and proficiency examinations for digital examiners.

3) Conduct the Tests in a Controlled Environment

Outside all the recommendations and standards set forth by NIST and the legal community, it only makes sense that a digital forensics examiner would perform an internal validation of the software and tools being used in the laboratory. In some cases these validations are arbitrary and can occur either in a controlled or uncontrolled environment. Since examiners are continuously bearing enormous caseloads and work responsibilities, consistent and proper validations sometimes fall through the cracks and are validated in a somewhat uncontrolled "on-the-fly" manner. It's also a common practice in digital forensics for examiners to "borrow" validations from other laboratories and fail to validate their own software and tools. Be very careful with letting this happen. Keep in mind that in order for digital forensics to be practicing true scientific principles, the processes used must be proven to be repeatable and reproducible. In order for this to occur, the validation should occur within a controlled environment within your laboratory with the tools that you will be using. If the examiner uses a process, software, or even a tool that is haphazard or too varied from one examination to the next, the science then becomes more of an arbitrary art. Simply put, validations not only protect the integrity of the evidence, they may also protect your credibility. As stated previously, using a repeatable, consistent, scientific method in drafting these validations is always recommended.

4) Validate the Test Results against Known and Expected

Results

At this point, testing is conducted against the requirements set forth for the software or tool in the previous steps. Keep in mind that results generated through the experimentation and validation stage must be repeatable. Validation should go beyond a simple surface scan when it comes to the use of those technologies in a scientific process. With that said, it is recommended that each requirement be tested at least three times. If there are any variables that may affect the outcome of the validation (e.g. failure to write-block, software bugs) they should be determined after three test runs. There may be cases, however, where more or fewer test runs may be required to generate valid results.

It's also important to realize that you are probably not the first to use and validate a particular software or tool, so chances are that if you are experiencing inconsistent results, the community may be experiencing the same results as well. Utilizing peer review may be a valuable asset when performing these validations. Organizations such as the High Technology Crime Investigation Association (HTCIA) and the International Association of Computer Investigative Specialists (IACIS) maintain active member e-mail lists for members that can be leveraged for peer review. There are also various lists and message boards pertaining to mobile phone forensics that can be quite helpful when validating a new mobile technology. In addition, most forensic software vendors maintain message boards for software, which can be used to research bugs or inconsistencies arising during validation testing.

Conclusion

Real world laboratory use, controlled internal tests utilizing scientific principles, and peer review should all be leveraged in a validation test plan. Sharing unique results with the digital forensics community at-large helps investigators, examiners, and even software and tool vendors ensure that current best practices are followed. As the field of digital forensics continues to grow and evolve as a science the importance of proper scientific validation will be more important than ever.

References

1. Brown, C. "Computer Evidence: Collection & Preservation." Hingham: Thomson/Delmar. 2006.
2. Carrier, B. "Digital Forensics Tool Testing Images." Accessed 06 Feb 2011. http://dftt.sourceforge.net/.
3. *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579 (1993).
4. High Technology Crime Investigation Association, Accessed 06 Feb 2011. www.htcia.org.
5. International Association of Computer Investigative Specialists, Accessed 06 Feb 2011. www.iacis.org.
6. Maras, MH. Computer Forensics: Cybercriminals, Laws, and Evidence. Sudbury: Jones & Bartlett. 2011.
7. 7. Marshall University Forensic Science Center-Digital Publications, Accessed 06 Feb 2011. http://forensics.marshall.edu/Digital/Digital-Publications.html.
8. NIST Computer Forensic Tool Testing Project. Accessed 06 Feb 2011. www.cftt.nist.gov.
9. Shroader, A. "How to Validate Your Forensic Tools." Orem: Paraben Corp. 2010.

***Josh Brunty** currently manages the digital forensics graduate program and the digital forensics research and casework laboratories at the Marshall University Forensic Science Center in Huntington, WV. Josh holds numerous certifications within the digital forensics discipline including: AccessData Certified Examiner (ACE), Computer Hacking Forensic Examiner (CHFI), Seized Computer Evidence Recovery Specialist (SCERS), and is certified in Information Assessment Methodology (NSA-IAM). He has developed a variety of digital forensics training curriculum; including past recertification scenarios/exams for the International Association of Computer Investigative Specialists (IACIS). Josh is an active member of the Mid-Atlantic Association of the High Technology Crime Investigation Association (HTCIA) and the Digital-Multimedia Sciences section of the American Academy of Forensic Sciences (AAFS). He can be reached at josh.brunty@marshall.edu.*

Exhibit E: Software Reliability Tutorial

(extracted pages only)

Software Reliability

Lou Gullo

Jon Peterson

Raytheon Company

Raytheon

Customer Success Is Our Mission

Software Failures

- Specification errors
  - Typically the largest source of failure
  - Ambiguous requirements
- Errors in design of code
  - Incorrect interpretation of the spec
  - Incomplete interpretation of the spec
  - Incorrect logic in the interpretation of the spec
  - Timing errors and race conditions
  - Shared data variables

Capability Maturity Model
SEI Levels

Level	Description of Organization
Level 1: Initial	Organizations lack effective project management; do not maintain a solid, stable environment …
Level 2: Repeatable	Organizations maintain policies and procedures for managing and developing ... Project planning based upon experience …
Level 3: Defined	Organizations have developed and documented a standard process for managing and developing software systems....
Level 4: Managed	Organizations set quantitative goals … use measurement instruments to collect process and product metrics.
Level 5: Optimizing	Organizations focus on continuous process improvement…

Capability Maturity Model
Fault Density at Delivery Studies

CMM LEVEL	FAULTS/KSLOC (Keene Data)	FAULTS/KSLOC (Caper Jones)	FAULTS/KSLOC (Herb Krasner)	Defect Plateau Level
V	0.5	0.5	0.5	1.5%
IV	1.0	1.4	2.5	3.0%
III	2.0	2.69	3.5	5.0%
II	3.0	4.36	6.0	7.0%
I	5.0	7.44	30	10.0%

- Fault density is in defects per thousand lines of code (KSLOC).
- Data represents average expected results gathered from several SEI rated companies.

CERTIFICATE OF SERVICE

I, J. Curtis Edmondson, hereby certify that on April 29, 2019, I electronically served the **REBUTTAL EXPERT REPORT TO STRIKE 3 HOLDING'S EXPERT REPORTS OF PAIGE AND BUNTING REGARDING RELIABILITY OF THE IPP INFRINGEMENT MONITORING SYSTEM**

by email and mail which will send notification of such filing to the following:

Lincoln D. Bandlow, *Admitted Pro Hac Vice*
Law Offices of Lincoln Bandlow, P.C.
1801 Century Park East, Suite 2400
Los Angeles, California 90067
Phone: 310-556-9580
Fax: 310 861-5550
Email: Lincoln@BandlowLaw.com

John C Atkin
THE ATKIN FIRM, LLC
55 MADISON AVE STE 400
MORRISTOWN, NJ 07960
973-285-3239
Email: JAtkin@AtkinFirm.com

Jeremy E. Roller, WSBA No. 32021
1218 Third Avenue, Suite 2100
Seattle, WA 98101
Telephone: (206) 428-3250 Fax: (206) 428-3251
jroller@aretelaw.com

Attorneys for Plaintiff Strike 3 Holdings LLC

Joshua L Turnham
THE LAW OFFICE OF JOSHUA L TURNHAM PLLC
214 E GALER ST ST 100
SEATTLE, WA 98102
206-395-9267
Fax: 206-905-2996
Email: joshua@turnhamlaw.com
Attorney for Non-Party

By: /s/ J. Curtis Edmondson
J. Curtis Edmondson